Online Privacy Law
(2017 Update)

Australia • Canada • European Union • France • Germany
Israel • Italy • Japan • Netherlands • Portugal
Spain • Sweden • United Kingdom

December 2017

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

This report is provided for reference purposes only.
It does not constitute legal advice and does not represent the official opinion of the United States Government. The information provided reflects research undertaken as of the date of writing.
It has not been updated.

Contents

Introduction 1

Non-EU Countries

Australia 2

I. Introduction 2
II. Legislative Changes 5
  A. Privacy Amendment (Enhancing Privacy Protection) Act 2012 5
  B. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 8
  C. Privacy Amendment (Notifiable Data Breaches) Act 2017 8
III. Court Decision Relating to "Revenge Porn" 9
IV. Guidance and Studies Related to Online Privacy 9
V. "Attitudes to Privacy" Surveys 10

Canada 11

I. Recent Reforms and Amendments to Canada's Privacy Laws 11
II. Changes Made by the Digital Privacy Act 12
  A. Consent Requirements 12
  B. Scope of Application 13
  C. Other Exceptions 14
  D. Data Breach Notification 15
  E. Enhanced Powers of the Commissioner 15

Israel 17

I. Privacy Protection (Data Security) Regulations 17
  A. Databank Definitions Document 17
  B. Groups of Databanks 18
  C. Protection Procedures 19
  D. Systems Specification and Risk Analysis 19
  E. Physical, Environmental, and Personnel Security 20
  F. Telecommunications 20
II. Protection of Children's Privacy 20
III. Protection of Prisoners' Biometric Voice Recognition 21

Japan 23

I. Overview 23
  A. Laws 23
  B. Personal Information 24
  C. Right to Privacy 25
  D. Government's Roles 25

II. Protection of Personal Information Under the APPI 26
A. Businesses Handling Personal Information 26
B. Purpose of Utilization and Requirement for Consent 27
C. Disclosure to the Data Subject 28
D. Transfer to a Third Party 29
E. Complaints and Requests to Businesses 30
F. Certified Personal Information Protection Organization 31
G. Criminal Penalty for Data Theft 32
III. Unauthorized Access to Computers 32
IV. Right to Be Forgotten 32
V. PrivacyMark 33

EU Countries

European Union 35

I. Introduction 35
II. Legal Framework 38
A. General Data Protection Regulation 38
B. The ePrivacy Directive 46
C. Proposal for an ePrivacy Regulation 47

France 50

Germany 52

I. EU Cookie Directive 52
II. Data Retention 53
III. General Data Protection Regulation 55

Italy 57

Netherlands 59

I. Constitution 60
II. Laws 61
A. Amendments to the Personal Data Protection Act 61
B. Telecommunications Act 67
C. Data Breach Notification Rules 68
D. 2017 Act on Intelligence and Security Services 70
E. Data Retention Act Voided 72
III. Other Developments 72

Portugal 74

Spain 75

Sweden 79

I. Introduction 79
II. Legislative Change 80
  A. Implementation of the Data Retention Directive 80
  B. Adoption of Secret Surveillance Measures 80
  C. Personal Data Act 80
  D. New Rules on Sharing Personal Information Within the EU 81
  E. Changes to LEK 81
III. ECJ Limits Swedish Retention Provisions 81
IV. Domestic Case Law 83
V. Guidance 83
VI. Information Held by the Government 83
  A. Transfer of Private Information 83
  B. Government Sale of Personal Information 84
VII. Right to Be Forgotten 84
VIII. Outlook: The Swedish Constitution and GDPR 85

United Kingdom 86

I. Introduction 86
II. Retention of Data 86
  A. Retention Notice to Telecommunications Operator 87
  B. Type of Data to Be Retained 88
  C. Duration of Mandatory Retention of Data 88
  D. Cost of Retention 89
III. Sanctions for Regulatory Violations 89
IV. Protection of Minors and Facebook 90
V. Collection, Storage, and Use of Personal Data by Online Media or Services 90
VI. European Union's Data Protection Directive 90

Introduction

Peter Roudik
Assistant Law Librarian of Congress for Legal research

In 2012, the Law Library of Congress issued two reports reviewing how the right to personal data protection and the right to privacy on the web are regulated by the European Union and in twelve individual countries with highly developed digital infrastructures. The reports looked at European Union directives and regulations and the domestic laws of a number of jurisdictions both within and outside of the EU. This report updates the prior reports with new legal developments through December 2017.

Since 2012, many reforms in the field of online privacy have been initiated and implemented in all the jurisdictions previously surveyed. The EU revised its entire legislative framework for the protection of personal data. The EU General Data Protection Regulation entered into force and new ePrivacy legislation has been proposed. As of May 2018, European norms will become directly applicable in the Member States, although derogations for national legislation are possible in certain areas.

The newly updated country surveys for the EU Member States included in the prior reports analyze this overarching European legislation and summarize changes in domestic legislation adopted over the the past five years. The country surveys included in this study allow one to compare the details of how individual nations adapt international legal rules, assess powers granted to authorities in charge of monitoring the implementation of national data protection information, and analyze particular issues, which are specific for each country. Among other issues, the individual country surveys provide examples of legal measures undertaken to secure the country's transition to a "digital republic" (France), efforts to protect data at the company level (Germany), new procedures for breach notifications (Netherlands), and attempts to make government information more easily accessible (Italy). Those surveys also illustrate how countries analyze the impact of technological advancements on national criminal legislation (Spain), review the legality of investigative authorities to access data retained by telecommunications providers (United Kingdom) and the right of government agencies to sell collected personal information (Sweden), assess government attempts to protect minors when they engage in online activities (France, United Kingdom), and evaluate the impact of the *Google v. Spain* decision on the development of national data transfer legislation (EU countries).

Surveys of significant legal developments in Australia, Canada, Israel, and Japan provide an example of how non-EU Member States have amended their national data and online privacy protection legislative frameworks over the past five years to meet present-day challenges and concerns.

Non-EU Countries

Australia

Kelly Buchanan
Chief, Foreign, Comparative, and
International Law Division I

SUMMARY There have been a number of significant developments in Australia's legal framework related to privacy, including online privacy, in the past five years. Major reforms to the Privacy Act 1988 (Cth) were enacted at the end of the 2012 and came into effect in 2014, including changes to the principles related to the cross-border disclosure of information and direct marketing. In addition, a new data retention system was established, becoming fully effective in early 2017, with internet service providers required to retain certain data about online communications that can then be accessed by government agencies for law enforcement and national security purposes. A further legislative change in 2017 established a requirement for entities covered by the Privacy Act to notify affected individuals and the Information Commissioner of data breaches.

In addition to the legislative changes, the Office of the Australian Information Commission has produced new guidance documents, participated in international studies related to online privacy, and conducted surveys regarding attitudes to privacy among members of the public. There has also been ongoing discussion regarding civil redress for breaches of privacy, including a court case involving "revenge porn" that saw the respondent held liable for breach of confidence. The Australian government has indicated, however, that it does not support the introduction of a new statutory cause of action for invasion of privacy.

I. Introduction

During the period from 2012 to 2017, several significant legislative changes were made in Australia in relation to privacy law, with implications for online privacy.

As noted in the Law Library of Congress report on online privacy, published in 2012,[1] the Australian government had at that time introduced the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).[2] The bill included provisions that would implement more than half of the Australian Law Reform Commission's (ALRC's) recommendations contained in its 2008 report on reforming privacy law. The bill was subsequently enacted at the end of 2012 and the amendments to the Privacy Act 1988 (Cth) came into effect in March 2014.[3]

---

[1] KELLY BUCHANAN, ONLINE PRIVACY LAW: AUSTRALIA (Law Library of Congress, June 2012), https://www.loc.gov/law/help/online-privacy-law/australia.php.

[2] *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, PARLIAMENT OF AUSTRALIA, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813 (last visited Nov. 14, 2017), *archived at* https://perma.cc/5RWC-934K; Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), https://www.legislation.gov.au/Details/C2015C00053, *archived at* http://perma.cc/5S67-3FBK.

[3] *See* Kelly Buchanan, *Australia: New Privacy Law Comes into Effect*, GLOBAL LEGAL MONITOR (Mar. 21, 2014), https://www.loc.gov/law/foreign-news/article/australia-new-privacy-law-comes-into-effect/.

Following those reforms, there was considerable debate about a proposal to establish a requirement for telecommunications service providers, including internet service providers, to retain certain communications data that could then be accessed for law enforcement or national security purposes. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)[4] was enacted in in April 2015 and the implementation period ended in April 2017, at which time all service providers were required to be fully compliant with the legislation.[5]

A further development in 2017 was the passage of the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth).[6] This legislation implements recommendations that the Parliamentary Joint Committee on Intelligence and Security made in the context of its consideration of the data retention bill, as well as recommendations of the ALRC in its 2008 report.[7]

Also during this period, in 2014, the ALRC completed an inquiry into the protection of privacy in the digital era, which addressed "both prevention and remedies for serious invasions of privacy."[8] However, the current government has indicated that it does not support a tort of invasion of privacy, which the ALRC recommended establishing through a new statutory cause of action.[9] Such a recommendation was also included in the ALRC's 2008 report, and similar

---

[4] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, PARLIAMENT OF AUSTRALIA, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r5375 (last visited Nov. 14, 2017), *archived at* https://perma.cc/XL6L-29K2; Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), https://www.legislation.gov.au/Details/C2015A00039, *archived at* https://perma.cc/9ZUZ-PGMC. *See also* Kelly Buchanan, *Australia: Committee Report on Data Retention Bill Released*, GLOBAL LEGAL MONITOR (Mar. 4, 2015), http://www.loc.gov/law/foreign-news/article/australia-committee-report-on-data-retention-bill-released/.

[5] Attorney General's Department, *Data Retention Implementation Period Ends on 13 April 2017: What Service Providers Should Know* (Mar. 22, 2017), https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/Fact-sheet-data-retention-implementation-period.pdf, *archived at* https://perma.cc/8LMM-95TM.

[6] Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), https://www.legislation.gov.au/Details/C2017A00012, *archived at* https://perma.cc/R4MT-RHVG. *See also* Kelly Buchanan, *Australia: Bill Passed Requiring Notification of Data Breaches*, GLOBAL LEGAL MONITOR (Feb. 15, 2017), http://www.loc.gov/law/foreign-news/article/australia-bill-passed-requiring-notification-of-data-breaches/.

[7] *Privacy Amendment (Notifiable Data Breaches) Bill 2016*, PARLIAMENT OF AUSTRALIA, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747 (last visited Nov. 14, 2017), *archived at* https://perma.cc/7CKD-WQGS.

[8] *Serious Invasions of Privacy*, AUSTRALIAN LAW REFORM COMMISSION (ALRC), https://www.alrc.gov.au/inquiries/invasions-privacy (last visited Nov. 14, 2017), *archived at* https://perma.cc/BH4Y-2473; ALRC, SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA: FINAL REPORT (ALRC Report 123, June 2014), https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf, *archived at* https://perma.cc/X8XU-BUEP.

[9] *See ALRC Report on Serious Invasions of Privacy in the Digital Era*, KING & WOOD MALLESONS (Sept. 3, 2014), http://www.kwm.com/en/au/knowledge/insights/alrc-report-on-serious-invasions-of-privacy-in-the-digital-era-20140903, *archived at* https://perma.cc/W6YX-QY2Y; Normann Witzleb, *It's Time for Privacy Invasion to be a Legal Wrong*, THE CONVERSATION (Sept. 4, 2014), https://theconversation.com/its-time-for-privacy-invasion-to-be-a-legal-wrong-31288, *archived at* https://perma.cc/UW56-RJGG.

recommendations were made in 2009 by the New South Wales Law Reform Commission[10] and in 2010 by the Victorian Law Commission.[11] In 2016, the first bill in Australia related to remedies for serious invasions of privacy was introduced by a member of parliament in New South Wales,[12] following an inquiry conducted by a parliamentary committee.[13] The bill lapsed at the end of that year.

In the absence of a specific cause of action for breach of privacy, plaintiffs may be able to utilize other actions in certain situations. For example, in a 2015 "revenge porn" case, the court found that the respondent was liable for breach of confidence.[14]

Other discussions relevant to online privacy have taken place within the federal government. For example, in 2013, the Australian Communications and Media Authority released a paper that discusses developments in the digital data environment and their impact on privacy.[15] It also published other papers related to mobile applications, cloud services, and near field communications.[16]

---

[10] *See Privacy*, NSW LAW REFORM COMMISSION, http://www.lawreform.justice.nsw.gov.au/Pages/lrc/lrc_completed_projects/lrc_privacy.aspx (last updated Feb. 23, 2017), *archived at* https://perma.cc/JWR5-G2ZN; NSW LAW REFORM COMMISSION, INVASION OF PRIVACY (Report 120, Apr. 2009), http://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-120.pdf, *archived at* https://perma.cc/MB3B-RWXJ.

[11] *Surveillance in Public Places*, VICTORIAN LAW REFORM COMMISSION, http://www.lawreform.vic.gov.au/all-projects/surveillance-public-places (last updated Nov. 14, 2017), *archived at* https://perma.cc/X5V4-QEMK; *Keeping Privacy Lives Private*, VICTORIAN LAW REFORM COMMISSION (Oct. 1, 2011), http://www.lawreform.vic.gov.au/publications-and-media/journal-articles/keeping-private-lives-private, *archived at* https://perma.cc/N56J-VHHC.

[12] *Civil Remedies for Serious Invasions of Privacy Bill 2016*, PARLIAMENT OF NEW SOUTH WALES, https://www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=3307 (last visited Nov. 15, 2017), *archived at* https://perma.cc/SPY8-TFVK.

[13] *Remedies for Serious Invasion of Privacy in New South Wales*, PARLIAMENT OF NEW SOUTH WALES, https://www.parliament.nsw.gov.au/committees/inquiries/Pages/inquiry-details.aspx?pk=1877 (last visited Nov. 15, 2017), *archived at* https://perma.cc/NHU7-XP2N.

[14] *See* Kelly Buchanan, *Australia: Damages Awarded in Revenge Porn Case*, GLOBAL LEGAL MONITOR (Feb. 12, 2015), http://www.loc.gov/law/foreign-news/article/australia-damages-awarded-in-revenge-porn-case/.

[15] *Privacy and Digital Data – Emerging Issues*, AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, https://www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/privacy-and-digital-data-emerging-issues (last updated Oct. 21, 2013), *archived at* https://perma.cc/9QPN-PFAD.

[16] *Id.*

II. Legislative Changes

A. Privacy Amendment (Enhancing Privacy Protection) Act 2012

1. Key Changes

The "significant reforms" to the Privacy Act 1988 (Cth) contained in the 2012 Amendment Act

- create a single set of Australian Privacy Principles (APPs) applying to both Australian Government agencies and the private sector. These principles replaced the Information Privacy Principles and National Privacy Principles and set out the standards, rights and obligations for collecting, handling, holding, accessing, using, disclosing and correcting personal information
- introduce more comprehensive credit reporting for consumer credit, improved privacy protections and more logical, consistent and simple language
- strengthen the functions and powers of the Australian Information Commissioner to resolve complaints, use external dispute resolution services, conduct investigations and promote compliance
- create new provisions on privacy codes and the credit reporting code, including codes that are binding on specified agencies and organisations.[17]

The thirteen Australian Privacy Principles (APPs) are contained in schedule 1 of the Privacy Act 1988 (Cth) and are divided into five parts:

> Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.
>
> Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.
>
> Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.
>
> Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.
>
> Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.[18]

---

[17] *Privacy Act Amendments*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/PrivacyActamendments.aspx (last visited Nov. 15, 2017), *archived at* https://perma.cc/UG2Q-KRXG.

[18] Privacy Act 1988 (Cth), sch 1, Overview of the Australian Privacy Principles, https://www.legislation.gov.au/Details/C2017C00283, *archived at* https://perma.cc/KC3Y-NPDU. For a list of the principles, *see Privacy Fact Sheet 17: Australian Privacy Principles*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC), https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles (last updated Jan. 2014), *archived at* https://perma.cc/AVT4-LF9G.

Some of the new APPs differ from the previous Information Privacy Principles (which applied to Australian government agencies) and National Privacy Principles (which applied to private sector entities with annual turnover of more than AU$3 million, as well as those that handle certain information or opt in).[19] This includes "APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information."[20]

Following the passage of the 2012 Amendment Act, new regulations were developed, the Privacy Regulation 2013 (Cth), which came into effect at the same time as the amendments.[21]

2. Cross-Border Disclosure of Personal Information

APP 8, on cross-border disclosure of information, along with section 16C of the Privacy Act 1988 (Cth), establishes a framework that follows the "accountability approach" to this issue that was adopted by the APEC Privacy Framework in 20014, shifting away from the "adequacy approach" adopted by the European Union, which had previously been reflected in the Act.[22] The new approach "generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information."[23] The Office of the Australian Information Commissioner (OAIC) guidance on this APP includes examples relevant to online privacy, stating that an APP entity will be considered to have "disclosed" personal information about an individual if it "publishes the personal information on the internet, whether intentionally or not, and it is accessible to an overseas recipient."[24] It also covers the situation where "an APP entity engages a contractor located overseas to perform services on its behalf" and provides it with personal information. For example, a disclosure would include the scenario where "an Australian based retailer outsources the processing of online purchases through its website to an

[19] For comparisons between the APP and NPP, and the APP and IPP, *see Australian Privacy Principles and National Privacy Principles – Comparison Guide*, OAIC (Apr. 2013), https://www.oaic.gov.au/agencies-and-organisations/guides/australian-privacy-principles-and-national-privacy-principles-comparison-guide, *archived at* https://perma.cc/QGH6-6J5L, *and Australian Privacy Principles and Information Privacy Principles – Comparison Guide*, OAIC (Apr. 2013), https://www.oaic.gov.au/agencies-and-organisations/guides/australian-privacy-principles-and-information-privacy-principles-comparison-guide, *archived at* https://perma.cc/B49S-SNW7.

[20] *Privacy Reforms*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/Privacyreforms.aspx (last visited Nov. 15, 2017), *archived at* https://perma.cc/958K-MVF3.

[21] Privacy Regulation 2013 (Cth), https://www.legislation.gov.au/Details/F2017C00191, *archived at* https://perma.cc/3ABR-2DHX.

[22] Parliament of Australia, Privacy Amendment (Enhancing Privacy Protection) Bill 2012: Explanatory Memorandum 70, http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf, *archived at* https://perma.cc/5Z7D-FLSH.

[23] *APP Guidelines, Chapter 8: APP 8 – Cross-Border Disclosure of Personal Information*, OAIC (version 1.1, Mar. 2015), https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information, *archived at* https://perma.cc/48Z5-U8NH.

[24] *Id.*

overseas contractor and, in order to facilitate this, provides the overseas contractor with personal information about its customers."[25]

There are exceptions to the requirement in APP 8.1 to take "reasonable steps" to ensure an overseas recipient does not breach the APPs. If the overseas recipient of the information is subject to a law that protects information in a "substantially similar" way to the APPs, and mechanisms can be accessed by the individual to enforce that protection, then the APP entity in Australia does not need to comply with APP 8.1. An APP entity may also not need to comply with APP 8.1 if it "expressly informs the individual that if they consent to the disclosure, this principle will not apply," and the individual consents to the disclosure. Other exceptions relate to, for example, law enforcement activities, protection of health and life, and compliance with other laws and regulations.[26]

3. Direct Marketing

The new APP 7 establishes a separate, general prohibition on direct marketing. Previously, the use or disclosure of information for direct marketing purposes was an exception in one of the NPPs. Under the reforms, entities "may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met."[27]

4. Functions and Powers of the Information Commissioner

As noted above, the amendments to the Privacy Act in 2012 were intended to "improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations."[28] The amendments "also restructure relevant provisions dealing with the powers and functions of the Commissioner to improve clarity and consistency in the provisions."[29]

The functions of the Commissioner are now divided into guidance-related functions, monitoring-related functions, advice-related functions, and any functions conferred by the Act or other legislation, including investigating complaints about actions or practices that may interfere with the privacy of individuals.[30]

---

[25] *Id.*

[26] *Id.*

[27] *Australian Privacy Principles and National Privacy Principles – Comparison Guide*, *supra* note 19; Explanatory Memorandum, *supra* note 22, at 81–2 & 216–7.

[28] Explanatory Memorandum, *supra* note 22, at 4–5.

[29] *Id.*

[30] Privacy Act 1988 (Cth) pts IV & V.

B. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

Under the data retention system established by amendments to the Telecommunications (Interception and Access) Act 1979 (Cth),[31] telecommunications service providers, including internet service providers, are "required to retain a particular set of telecommunications data for at least two years."[32] The type of data that must be retained includes "information about a communication rather than the content or substance of a communication."[33] This means, for example, that for emails, the retention requirements apply to "information such as the relevant email addresses and when it was sent—not the subject line of the email or its content."[34] Furthermore, the legislation "does not require companies to retain data that may amount to a person's web-browsing history."[35] Companies are also not required to keep data about a person's use of social media.[36]

The legislation enables agencies to access the data as part of serious criminal or national security investigations, subject to various safeguards.

C. Privacy Amendment (Notifiable Data Breaches) Act 2017

The new system for notifiable data breaches, which will come into effect in February 2018,[37] requires "government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm."[38] The notice must include recommendations that such individuals should take in response to the breach.[39] The OAIC must also be informed of data breaches and can determine what further action is required. The Commissioner has the authority to direct an entity to notify individuals if it has not done so.

---

[31] Telecommunications (Interception and Access) Act 1979 (Cth), https://www.legislation.gov.au/Details/C2017C00308, *archived at* https://perma.cc/DFE3-FPFN.

[32] *Data Retention*, ATTORNEY GENERAL'S DEPARTMENT, https://www.ag.gov.au/dataretention (last visited Nov. 15, 2017), *archived at* https://perma.cc/AWQ4-LQ7C.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Frequently Asked Questions about the Data Retention Obligations*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx (last visited Nov. 15, 2017), *archived at* https://perma.cc/TY54-6L6C.

[37] Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), s 2.

[38] Press Release, OAIC, Mandatory Data Breach Notification (Feb. 13, 2017), https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification#mandatory-data-breach-notification, *archived at* https://perma.cc/7NLN-MVDX.

[39] *Notifiable Data Breaches: Resources for Businesses and Agencies*, OAIC, https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/ (last visited Nov. 15, 2017), *archived at* https://perma.cc/6EJA-8EGD.

III. Court Decision Relating to "Revenge Porn"

In early 2015, the Supreme Court of Western Australia issued a decision in which it found in favor of a plaintiff in a "revenge porn" case involving the posting of private images on Facebook.[40] The plaintiff relied on a breach of confidence cause of action, which involves the unauthorized use of confidential information, as there is no statutory or common law tort of invasion of privacy in Australia. The court exercised its equitable jurisdiction in issuing an injunction against further disclosure of the photographs at issue, and also ordered that the defendant pay compensation.[41]

IV. Guidance and Studies Related to Online Privacy

In the past five years, the OAIC has produced various guidance documents related to the amended Privacy Act and developments in online technology, and has participated in international studies regarding the protection of privacy online. These include the following:

- The 2015 *Guide to Securing Personal Information*,[42] which is intended to be read alongside the *Australian Privacy Principles Guidelines*.[43] The *Guide* is intended for use by entities covered by the Privacy Act and will be referred to by the OAIC in undertaking its functions. The *APP Guidelines* outline mandatory requirements contained in the APPs, how the APPs will be interpreted by the OAIC, and matters that the OAIC may take into account when exercising its functions.
- A "better practice guide" for mobile app developers, published in 2014, which is intended to help developers embed better privacy practices in their products and services and help those operating in the Australian market to comply with Australian privacy law.[44]
- An August 2013 press release on the results of a "privacy sweep" of the websites most used by Australians, which was part of the "first international internet privacy sweep, an initiative of the Global Privacy Enforcement Network (GPEN)."[45] As part of the sweep, "[a]lmost 50 website privacy policies were assessed for accessibility, readability and content," as well as being assessed against new transparency criteria in the Privacy Act.[46]

---

[40] *Wilson v Ferguson* [2015] WASC 15 (6 January 2015), http://www8.austlii.edu.au/cgi-bin/sign.cgi/au/cases/wa/WASC/2015/15, *archived at* https://perma.cc/M5PB-DXSS.

[41] *Id.* ¶ 2.

[42] *Guide to Securing Personal Information*, OAIC (Jan. 2015), https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information, *archived at* https://perma.cc/87BN-AVNC.

[43] *APP Guidelines*, OAIC (last updated Apr. 1, 2015), https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/, *archived at* https://perma.cc/NCN6-BK9P.

[44] *Guide for Mobile App Developers*, OAIC (Sept. 2014), https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers, *archived at* https://perma.cc/L4KT-624R.

[45] Press Release, OAIC, Privacy Commissioner: Website Privacy Policies are too Long and Complex (Aug. 14, 2013), https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex, *archived at* https://perma.cc/VYZ8-K2ER.

[46] *Id.*

- A September 2016 press release regarding a global sweep of the "Internet of Things," which was also a GPEN initiative. The Australian Privacy Commissioner "found that the Australian businesses assessed as part of the sweep generally lacked clear information for customers about how their personal information was being managed — with more than half failing to adequately explain how personal information was collected, used and disclosed."[47]

V. "Attitudes to Privacy" Surveys

The OAIC again ran the "Community Attitudes to Privacy" survey project in 2013 and 2017,[48] having conducted similar surveys periodically since 1990.[49] In the most recent survey, among the biggest privacy risks that respondents identified were online services, including social media sites. The report notes that "[t]he majority of Australians claim to be more concerned about the privacy of their personal information when using the internet than five years ago (69%), a consistent finding compared to the last two surveys. A new question this year revealed that more than eight in ten (83%) believe the privacy risks are greater when dealing with an organisation online compared with other means."[50]

However, despite their concerns about online privacy, respondents indicated that they did not use some of the privacy protections available: "Over three in five (61%) Australians do not regularly read online privacy policies and about half do not regularly shred documents (50%), clear their browsing history (50%), or adjust their privacy settings on social media sites (43%)."[51]

---

[47] Press Release, OAIC, Privacy Commissioners Reveal the Hidden Risks of the Internet of Things (Sept. 23, 2016), https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things, *archived at* https://perma.cc/D4BX-9K2A.

[48] *Community Attitudes*, OAIC, https://www.oaic.gov.au/engage-with-us/community-attitudes/ (last visited Nov. 15, 2017), *archived at* https://perma.cc/3DTD-48DE.

[49] *Australian Community Attitudes to Privacy Survey 2017*, OAIC (https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017 (last visited Nov. 15, 2017), *archived at* https://perma.cc/ZS9Z-JGRB.

[50] *Id.*

[51] *Id.*

Canada

Tariq Ahmad
Foreign Law Specialist

SUMMARY The Digital Privacy Act, which received Royal Assent in June 2015, brought a number of changes to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)—the federal privacy law applicable to the private sector. PIPEDA was amended to specify what constitutes valid consent for the collection, use, or disclosure of personal information. Moreover, the scope of application of the Act was changed in a number of ways by introducing a several new definitions and exemptions that allow personal information to be collected, used, or disclosed without consent, such as for business transactions. The Digital Privacy Act also amended PIPEDA to introduce mandatory data breach notification requirements. In addition, the Act included a number of provisions that enhance the powers of the Privacy Commissioner, including a new provision that allows the Privacy Commissioner to enter into compliance agreements aimed at ensuring organizations comply with PIPEDA.

I. Recent Reforms and Amendments to Canada's Privacy Laws

Canada has a number of laws at the federal and provincial levels that relate to the protection of personal information. The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law applicable to the private sector.[1] Section 29 of PIPEDA requires Parliament to review Part 1 of the Act, which deals with data protection, every five years.[2] In May 2010, the Government introduced Bill C-29,[3] which contained a number of amendments to the Act "flowing from the first PIPEDA review."[4] This legislation died on the order paper, but was reintroduced in September 2011 as Bill C-12.[5] This Bill also was not passed.

The federal government's most recent, and ultimately successful, attempt to amend PIPEDA was by way of Bill S-4. This measure incorporated a number of provisions from Bill C-12 and included recommendations made by witnesses during the 2012 privacy and social media study conducted by the House of Commons Standing Committee on Access to Information, Privacy

---

[1] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html, *archived at* https://perma.cc/474H-3BTQ.

[2] *PIPEDA Review*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/ (last modified July 15, 2013), *archived at* https://perma.cc/MA4T-MN7Y.

[3] Bill C-29, Third Session, Fortieth Parliament, 59 Elizabeth II, 2010, http://www.parl.ca/DocumentViewer/en/40-3/bill/C-29/first-reading, *archived at* https://perma.cc/ZW54-WFXP.

[4] *PIPEDA Review*, *supra* note 2.

[5] Bill C-12 First Session, Forty-first Parliament, 60 Elizabeth II, 2011, http://www.parl.ca/DocumentViewer/en/41-1/bill/C-12/first-reading, *archived at* https://perma.cc/62YS-R332.

and Ethics, and a position paper by the Office of the Privacy Commissioner entitled *The Case for Reforming the Personal Information Protection and Electronic Documents Act*.[6]

Bill S-4 was passed as the Digital Privacy Act[7] and received Royal Assent on June 2015.[8] The Act made a number of significant amendments to PIPEDA.[9]

II. Changes Made by the Digital Privacy Act

A. Consent Requirements

The Digital Privacy Act amended PIPEDA to specify what constitutes valid consent for the collection, use, or disclosure of personal information by adding the following section:

> **Valid consent**
>
> **6.1** For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting[10]

Industry Canada under the Harper Government explained the purpose the inclusion of this new consent requirement as follows: "The new measures also establish stronger rules to ensure that vulnerable Canadians, particularly children, fully understand the potential consequences when companies ask to collect and use their personal information. Companies will need to communicate these requests in clear and simple language for the target audience."[11]

According to lawyer Bradley J. Freedman,

> [t]he "valid consent" requirement is an extension of the fundamental principle of "meaningful" consent, which requires that consent be reasonably informed. Organizations should critically assess and adjust their privacy explanations (e.g. privacy policies, notifications and reminders) to adequately and accurately explain, in ways that

[6] Dara Lithwick, Legal and Social Affairs Division, Parliamentary Information & Research Service, *Legislative Summary of Bill S-4: An Act to Amend the Personal Information Protection and Electronic Documents Act and to Make a Consequential Amendment to Another Act* (June 11, 2014), https://lop.parl.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf, *archived at* https://perma.cc/V59E-E23C.

[7] Digital Privacy Act, S.C. 2015, c. 32, http://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html, *archived at* https://perma.cc/EKW7-7MMA.

[8] *The Digital Privacy Act and PIPEDA*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, (Nov. 2015), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/02_05_d_63_s4/, *archived at* https://perma.cc/S5KF-DDAN.

[9] *Id*.

[10] Digital Privacy Act (adding § 6.1 to PIPEDA).

[11] *Harper Government Introduces New Law to Protect the Personal Information of Canadians Online*, GOVERNMENT OF CANADA (Apr. 8, 2014), https://www.canada.ca/en/news/archive/2014/04/harper-government-introduces-new-law-protect-personal-information-canadians-online.html, *archived at* https://perma.cc/547A-973N.

> members of the organization's target market can reasonably be expected to understand, the nature, purpose and consequences of the organization's collection, use and disclosure of personal information.[12]

B. Scope of Application

1. Business Contact Information

Prior to the amending legislation, PIPEDA had "excluded an employee's 'name, title or business address or telephone number' from the definition of "personal information' ".[13] According to the Office of the Privacy Commissioner of Canada, the Digital Privacy Act (DPA) introduces changes to make clear that "PIPEDA does not apply in respect of business contact information." The DPA replaces the definition of "personal information" in section 2(1) of PIPEDA to mean "information about an identifiable individual."[14] Moreover section 2(1) also adds a separate definition of the term "business contact information," as follows:

> "business contact information" means any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address.[15]

In addition, section 4 of the DPA also then "uses this newly defined term in a specific 'business contact' exemption provision," which excludes from PIPEDA use of "business contact information" for the purpose of communicating or facilitating communications with an individual in relation to their employment, business or profession."[16]

2. Business Transaction Exemption

The Act also created a number of new exemptions under which "personal information can be collected, used or disclosed without consent."[17] One of the aims of the amending legislation is to "permit organizations, for certain purposes, to use and disclose, without the knowledge or consent of an individual, personal information related to prospective or completed business transactions."[18] This can only be done provided that certain conditions are met. PIPEDA was amended to add the following definition of a "business transaction," which includes

---

[12] Bradley J. Freedman, Borden Ladner Gervais LLP, *Digital Privacy Act – New Requirement for Valid Consent to Use Personal Information*, LEXOLOGY (June 25 2015), https://www.lexology.com/library/detail.aspx?g=fd17bab4-03da-4647-8a3c-2a5d96bbb2f5, *archived at* https://perma.cc/5EHV-D6B3.

[13] Dan Cooper, *Highlights of the Canada Digital Privacy Act 2015*, INSIDE PRIVACY (Covington & Burling LLP, June 24, 2015), https://www.insideprivacy.com/international/canada/highlights-of-the-canada-digital-privacy-act-2015/, *archived at* https://perma.cc/FR8L-K5N4.

[14] Digital Privacy Act § 2(1) (replacing the definition of "personal information" in subsec. 2(1) of PIPEDA).

[15] *Id.* § 2(3) (adding definition of "business contact information" in subsec. 2(1) of PIPEDA).

[16] Cooper, *supra* note 13.

[17] *The Digital Privacy Act and PIPEDA*, *supra* note 8.

[18] Digital Privacy Act, *summary*.

> *(a)* the purchase, sale or other acquisition or disposition of an organization or a part of an organization, or any of its assets;
> *(b)* the merger or amalgamation of two or more organizations;
> *(c)* the making of a loan or provision of other financing to an organization or a part of an organization;
> *(d)* the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization;
> *(e)* the lease or licensing of any of an organization's assets; and
> *(f)* any other prescribed arrangement between two or more organizations to conduct a business activity.[19]

The Digital Privacy Act also adds section 7.2 to PIPEDA, which establishes an exemption to nondisclosure absent consent for prospective and completed business transactions.[20] The Office of the Privacy Commissioner of Canada has described the scope of this exemption as follows:

> - Organizations that are parties to a prospective business transaction can only use and disclose the personal information if it is necessary to decide whether to proceed with or complete the transaction. In addition, the organization receiving personal information must enter into an agreement to use or disclose the information for the sole purpose of the transaction, to protect it, and to return or destroy the information if the transaction does not proceed.
> - If the transaction is completed, the parties have to enter into an agreement to limit the use or disclosure of the information to the purposes for which it was collected, to protect it, and give effect to any withdrawals of consent. In addition, the information must be necessary for carrying on the activity that was the object of the transaction and individuals must be notified their personal information has been transferred to a new owner.
> - These provisions do not apply to a business transaction which primarily involves the sale or lease of personal information.[21]

C. Other Exceptions

The Digital Privacy Act also allows organizations to disclose personal information without consent to another organization when the disclosure is for reasonable purposes of "investigating a breach of an agreement or contravention of a law that has been, is being or is about to be committed" or "detecting or suppressing fraud or . . . preventing fraud that is likely to be committed."[22] The Act also allows for "the collection, use and disclosure of personal information in witness statements without consent where 'necessary to assess, process, or settle an insurance claim.' "[23] Disclosures without consent are also allowed "to a government institution, individual's next of kin, or authorized representative . . . if necessary to identify an individual

[19] *Id*. § 2(3) (adding definition of "business transaction" in subsec. 2(1) of PIPEDA).

[20] Digital Privacy Act § 7 (amended by adding § 7.2 before § 8 of PIPEDA).

[21] *The Digital Privacy Act and PIPEDA*, *supra* note 8.

[22] *Id*.

[23] *Id*.

who is injured, ill or deceased."[24] Moreover, organizations such as banks now have "the authority to disclose personal information without consent to a government institution or an individual's next of kin or authorized representative when they have reasonable grounds to believe the individual 'has been, is or may be the victim of financial abuse.' "[25]

D. Data Breach Notification

The Digital Privacy Act amends PIPEDA to introduce mandatory data breach notification requirements. Section 10.1 of PIPEDA requires an organization to report to the Commissioner and to notify individuals if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the person.[26] PIPEDA provides a definition of "significant harm," which includes "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."[27] PIPEDA also includes a number of factors that are used to determine whether something amounts to a "real risk," including consideration of the sensitivity of the personal information involved in the breach, the probability that the personal information has been, is being or will be misused, and any other prescribed factor.[28]

These provisions are not yet in force due to a lack of subsidiary regulations, but in early September 2017 draft privacy breach regulations were published to allow for open comment for thirty days.[29]

E. Enhanced Powers of the Commissioner

The Digital Privacy Act also includes a number of provisions that enhance the powers of the Privacy Commissioner. The Office of the Privacy Commissioner of Canada outlines some of these changes as follows:

> **Compliance Agreements**
>
> - A new provision allows the Privacy Commissioner to enter into compliance agreements aimed at ensuring organizations comply with PIPEDA where the

[24] *Id.*

[25] *Id.*

[26] Digital Privacy Act § 10 (amended by adding section 10.1 of PIPEDA).

[27] *Id.*

[28] Karl Schober & Timothy M. Banks, Dentons, *Data Security and Breach Notification in Canada*, LEXOLOGY (Apr. 4, 2017), https://www.lexology.com/library/detail.aspx?g=a7378410-72cb-4d48-9f3f-4e4d1e748d7e, *archived at* https://perma.cc/MKH6-EWKT; Alex Cameron, Fasken Martineau DuMoulin LLP, *Digital Privacy Act: Mandatory Breach Notification and Other Important Changes to Canadian Privacy Law*, LEXOLOGY (June 24, 2015), https://www.lexology.com/library/detail.aspx?g=8129199e-9c0e-4837-ad15-233db6bcf442, *archived at* https://perma.cc/MVF2-DADV.

[29] Department of Industry, Breach of Security Safeguards Regulations, CANADA GAZETTE pt. I, vol. 151, no. 35 (Sept. 2, 2017), http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.php, *archived at* https://perma.cc/H2L6-ADZE.

Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of PIPEDA or a failure to follow a recommendation in Schedule I to the Act.

- Under a compliance agreement, an organization agrees to take certain actions to bring itself into compliance with PIPEDA. Entering into a compliance agreement would preclude the Privacy Commissioner from commencing or continuing a court application under PIPEDA in respect of any matter covered by the agreement.
- However, if an organization ultimately fails to live up to commitments in an agreement, the OPC could, after notifying the organization, either apply to the court for an order requiring the organization to comply with the terms of the agreement, or commence or reinstate court proceedings under PIPEDA as appropriate.[30]

Public Interest Disclosures

- PIPEDA's confidentiality provisions continue to apply, but the scope of what can be disclosed in the public interest has been broadened. The Commissioner may now make public any information that comes to his knowledge in the performance or exercise of his duties or powers under the Act if he deems that doing so is in the public interest. Previously, this discretion applied only to information "relating to the personal information management practices of an organization."[31]

[30] *The Digital Privacy Act and PIPEDA*, *supra* note 8.

[31] *Id*.

Israel

Ruth Levush
Senior Foreign Law Specialist

SUMMARY This report addresses legal developments in Israel in the area of online privacy protection from June 2012 to the present. These developments include the adoption of comprehensive Privacy Protection (Data Security) Regulations. In addition, primary legislation now provides for special procedures to protect data collected and stored information regarding children in foster care and in preschool programs. In the absence of primary legislation on the issue, an Attorney General Directive was also issued on a temporary basis to regulate procedures for the retrieval and storage of prisoners' biometric voice recognition data obtained with prisoners' consent for facilitation of telephone communications.

I. Privacy Protection (Data Security) Regulations

On April 5, 2017, Israel's Minister of Justice issued the Privacy Protection (Data Security) (PPDS) Regulations, 5777-2017.[1] The PPDS went into force on May 8, 2017.[2] The PPDS introduce detailed requirements for data protection by databank controllers and processors in both the public and private sectors.[3] The following are some of the PPDS's key provisions on the operation of databanks.

A. Databank Definitions Document

The PPDS Regulations require all databank owners to define and annually update their Databank Definitions Document (DDD) to include information on types of data included in the databank; methods of data collection; the purpose of data use; data transfer or use outside of Israel; data processing activities; main security risks and ways to address them; and names of the databank owner or possessor and of the person in charge of information security, if one has been appointed.[4]

---

[1] Privacy Protection Regulations (Data Security), 5777-2017 (PPDS), KOVETZ HATAKANOT [KT] [SUBSIDIARY LEGISLATION] 5777 No. 7809 p. 1022, available on the Ministry of Justice website, http://www.justice.gov.il/Units/Reshomot/publications/Pages/Regulations.aspx?WPID=WPQ7&PN=54 (in Hebrew; scroll down to No. 7809), *archived at* https://perma.cc/6UH6-KD6B. For a summary of the regulations see Ruth Levush, *Israel: Online Privacy Protection Regulations Adopted*, GLOBAL LEGAL MONITOR (June 14, 2017), http://www.loc.gov/law/foreign-news/article/israel-online-privacy-protection-regulations-adopted/, *archived at* https://perma.cc/QCU8-TJS3.

[2] PPDS § 22.

[3] Omer Tene, *Israel Enacts Landmark Data Security, Notification Regulations*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP), https://iapp.org/news/a/israel-enacts-landmark-data-security-notification-regulations/, *archived at* https://perma.cc/WX3H-4488.

[4] PPDS § 2.

B. Groups of Databanks

The PPDS Regulations divide databanks into four groups according to the level of information security they require: (1) databases not requiring a specific level of security, (2) databases requiring basic-level security, (3) databases requiring mid-level security, and (4) databases requiring high-level security.

1. Databases Not Requiring a Specific Level of Security

These databases are managed by an individual or by a corporation owned by an individual, and are accessible to that individual and to no more than two additional persons. Excluded from this category are databases whose primary objective is the collection of data for delivery to other entities as a business, including by targeted mail. According to a Ministry of Justice publication, "targeted mail" is mail that is directed at a person based on his/her belonging to a segment of the population, an affinity determined on the basis of one or more characteristics of persons whose names are included in a database.[5]

Databases that contain information on 10,000 persons or more, or information that is subject to professional confidentiality under the law or professional ethics, are similarly not included among those that do not require a specific level of security.[6]

2. Databases Requiring Basic-level Security

These are databases that are not managed by an individual, that are accessible by no more than ten persons, and that contain information that is exclusively used for administration of a business, excluding databases that contain information on a person's private life, political or religious affiliation, or biometric or confidential genetic characteristics.[7]

3. Databases Requiring Mid-level Security

Mid-level security is required for databases that are owned by a public body or that are principally intended "to collect data for delivery to another entity as a business, including by targeted mail,"[8] and that generally include sensitive information, such as medical, genetic, or biometric information, information on a person's private affairs, and information on a person's political or religious beliefs.[9]

---

[5] Questions and Answers on Registration of Databanks, ISRAELI LAW AND TECHNOLOGY AUTHORITY, http://www.justice.gov.il/Units/ilita/faq/Pages/faqregistration.aspx (in Hebrew; last visited Nov. 1, 2017) (scroll down to item 3), *archived at* https://perma.cc/C96G-67UK.

[6] PPDS § 1.

[7] *Id.*, App. 1, § 2.

[8] *Id.* § 1.

[9] *Id.*

4. Databases Requiring High-level Security

In general, high-level security is required for databases that would otherwise require mid-level security but include information on more than 100,000 people or are accessible by more than one hundred persons.[10]

C. Protection Procedures

Databank owners are required to establish specific procedures for data protection. Data protection procedures will be disclosed to and must be followed by access permit holders only to the extent needed for the performance of their jobs.[11] An access permit holder is defined as an individual who has obtained an access permit from the owner or possessor of a database to the databank's stored information, systems, or information or to a component needed for operation of or access to the databank.[12]

The databank owner must create a data protection procedures document that includes, among other information, instructions on the physical protection of the databank, information on access permit holders, and an identification of the possible security risks and responses that take into consideration the severity of a breach and the level of sensitivity of the data.[13] Supplemental information must be added by owners of databanks that are subject to mid- and high-level protections, to include references to means of identification and certification of those given access to the data, control of data use, instructions for the conduct of periodic audits, and backup procedures.[14]

D. Systems Specification and Risk Analysis

A databank owner must retain and keep updated a document that includes the databank structure and a list of its systems, including its infrastructure, telecommunications and security protection, operating system software, a diagram of the network on which the databank operates, and the connections among its different components. Special rules apply to databanks depending on their level of security. The document will be shared with access holders only to the extent needed.[15] At least once every eighteen months owners of high-level security databanks must conduct a survey of the databank's data security, analyze the security risks, and correct the errors identified. Such owners are also responsible for testing the susceptibility of the databank systems to internal and external security risks.[16]

---

[10] *Id.*, App. 2.

[11] *Id.* § 4(a)–(b).

[12] *Id.* § 1.

[13] *Id.* § 4(c).

[14] *Id.* § 4(d).

[15] *Id.* § 5(a)–(b).

[16] *Id.* § 5(c)–(d).

E. Physical, Environmental, and Personnel Security

Databank owners must ensure that the systems enumerated above are protected. Owners of mid- to high-level security databases must also control and document any entry to and exit from the databanks. The Regulations also require caution in the selection and placement of employees to operate databanks, with additional requirements applicable to mid- and high-level security databanks.[17]

F. Telecommunications

Databank owners may not connect databank systems to the internet or to any other public system without installing proper protection against unauthorized penetration of the system or against software capable of causing damage to hardware or other software. Moreover, the transfer of information from a databank on a public system or the internet must utilize common encryption methods. The identity of the user and his/her grant of permission to use the databank will be verified. Access to databanks at mid- and high-levels of security must be provided through a means that is subject to the exclusive control of the access permit holder.[18]

II. Protection of Children's Privacy

On March 6, 2016, the Knesset (Israel's Parliament) passed the Foster Care for Children Law, 5776-2016.[19] The Law declares that its objective is to recognize by legislation the rights of children in foster care and the obligations of the state to ensure protection of their welfare and their rights.[20] The Law contains a special provision requiring protection of confidentiality of information regarding children subject to restrictions to the extent necessary for protecting their well-being or the well-being of other children placed in foster care.[21]

Similar protection for privacy of children is expressed in the Council for Preschoolers Law, 5777-2017,[22] passed by the Knesset on July 26, 2017, with effect from February 7, 2018.[23] The Law declares its objectives as providing preschoolers (children from birth to first grade) with the care necessary to support their physical and mental health and development, addressing their

---

[17] *Id.* §§ 6–7.

[18] *Id.* § 14.

[19] Foster Care for Children Law, 5776-2016, SEFER HAHUKIM [SH] [BOOK OF LAWS (official gazette)] 5776 No. 2534 p. 586, as amended.

[20] *Id.* § 1.

[21] *Id.* § 14.

[22] Council for Preschoolers Law, 5777-2017, SH 5777 No. 2658 p. 1129, http://fs.knesset.gov.il/20/law/20_lsr_390426.pdf (in Hebrew), *archived at* https://perma.cc/2RFD-MLYH; *see also* Ruth Levush, *Israel: Establishment of the Council for Preschoolers*, GLOBAL LEGAL MONITOR (Oct. 19, 2017), https://www.loc.gov/law/foreign-news/article/israel-establishment-of-the-council-for-preschoolers/, *archived at* https://perma.cc/Q3EB-Z3BG.

[23] *Id.* § 21(a).

educational and social needs, and offering appropriate conditions for attaining equal opportunities in their adult lives.[24]

The Law establishes the Council for Preschoolers (CP) as a unit within the Ministry of Education tasked with collecting information and conducting research and analysis for achieving the goals prescribed by the Law.[25] The CP is authorized to request information on issues relating to preschoolers from any public office except for information on personal character, private matters, health, economic situation, professional training, beliefs, and opinions.[26]

III. Protection of Prisoners' Biometric Voice Recognition

AG Directive No. 3.1103 regulates the taking and storing of voice recognition samplings retrieved from telephone conversations of prisoners utilizing the prisons' telephone system, which is managed by a private company.[27] The Directive states that its provisions are temporary and are applicable until the adoption of primary legislation on the subject.[28]

The Directive provides that the phone system was designed to enable prison authorities to exercise control "for maintaining proper behavior and preventing misuse of the phone system by the prison population."[29] The system is based on technology that enables the use of telephones by a prisoner who has elected to provide his/her unique biometric voice recognition for identification as an alternative to using an individualized identification card.[30]

Voice recognition identification, according to the Directive, facilitates the use and acquisition of additional time segments for phone use by prisoners and eliminates the fear of theft or loss of a card.[31] Voice recognition may also be useful for implementation of any restrictions on phone use that are imposed on the prisoner by a court or the prison authority. It also ensures that a prisoner could not unlawfully use the identification card of another prisoner, thereby minimizing conflicts among prisoners.[32]

Addressing the requirements under the Privacy Protection Law, 5741-1981 (PPL),[33] which prohibits violating the privacy of a person without his/her consent, the Directive explains that the

---

[24] *Id.* § 1.

[25] *Id.* §§ 3–4 & 11.

[26] *Id.* § 11(b); Protection of Privacy Law § 7.

[27] Protection of Privacy (Sampling of Prisoners' Voice Recognition and its Storage in a Databank), Attorney General Directive No. 3.1103 (Dec. 22, 2014, updated Jan. 19, 2015) (hereinafter PPSPR), http://www.justice.gov.il/Units/YoezMespati/HanchayotNew/Seven/3.1103.pdf, *archived at* https://perma.cc/8NSZ-XQEX.

[28] *Id.* § 1.

[29] *Id.* § 1.

[30] *Id.* §§ 1–2.

[31] *Id.*

[32] *Id.* § 3.

[33] Privacy Protection Law, 5741-1981, SH 5741 No. 1011 p. 128.

legal basis for retrieving voice recognition is the prisoner's knowing consent to the retrieval. The prisoner has the option of not agreeing to voice recognition identification and instead using an identification card. To ensure free will the prisoner must be informed of the objectives of the voice recognition sampling and of its preservation in the databank, the alternative identification card to which the prisoner is entitled, and the ability to change his/her mind at any time and have the data erased from the databank.[34]

The consent for biometric voice recognition of prisoners who are minors (fourteen through seventeen years) must generally be given by both the minor and his/her parent or guardian. If a prisoner does not have legal capacity consent must be given by his/her guardian, and if the prisoner can understand, by the prisoner as well.[35]

In the absence of specific regulation by primary legislation, the general rules regarding the management of databases under the PPL apply. Considering the special characteristics of the data and the reasons for its retrieval, however, the Directive provides special provisions for data protection, access, confidentiality, security, and erasure.[36]

Similarly to other databanks regulated under the Criminal Procedure (Enforcement Authorities-Body Search and Retrieval of Identification Measures) Law, 5756-1996 (CPEA Law),[37] the databank for preservation of biometric identification exclusively relates to "a population of offenders or suspects under arrest."[38] The taking and preserving of biometric voice recognition in the context of prisoners' phone conversations, however, is not covered by the CPEA Law.[39]

Considering that the basis for taking voice recognition sampling and preservation is the prisoner's consent for the purpose of receiving telephone services, and not the CPEA Law, any use of data stored in the voice recognition databank, including transfers of information for use by public bodies exercising statutory authorities, is prohibited.[40]

The Prison Authority must consistently monitor implementation of the rules established by the PPL as well as by the Directive. It must require telephone system operators to consistently report on management of their databanks and on any irregular incidents, such as unauthorized disclosure of data, entry of unauthorized person to a place where the databank is stored, or any use in excess of authorization. The Prison Authority must also conduct entry testing of the databank every eighteen months to verify its compliance with data security.[41]

---

[34] PPSPR §4.

[35] *Id.*

[36] *Id.* §§ 5–7.

[37] Criminal Procedure (Enforcement Authorities- Body Search and Retrieval of Identification Measures) Law, 5756-1996, SH 5756 No. 1573 p. 136.

[38] PPSPR § 8.

[39] *Id.*

[40] *Id.*

[41] *Id.* § 9.

Japan

Sayuri Umeda
Foreign Law Specialist

SUMMARY The Act on the Protection of Personal Information (APPI), which applies to online privacy matters in Japan, was significantly amended in 2015. The amendments took effect on May 30, 2017. The APPI requires business operators handling personal information to specify the purpose for which personal information is utilized when they collect personal information. When such business operators acquire sensitive information, in principle, they must obtain the consent of the data subject. The consent of the data subject is also required in order to transfer information to a third party. With respect to retained personal data, a business operator handling the data must make available to data subjects the business's contact information, purpose of utilization of personal information, procedures for requesting corrections and disclosure, and information on filing complaints.

The Personal Information Protection Commission (PIPC) oversees the handling of personal information by businesses. The PIPC can require businesses that handle personal information to submit reports and materials, and PIPC employees can visit businesses in order to interview persons handling personal information and inspect business records.

Unauthorized access to a computer is prohibited under the Act on the Prohibition of Unauthorized Computer Access.

I. Overview

A. Laws

The Act on the Protection of Personal Information (APPI)[1] contains basic data protection policies applicable to the private sector. The rules are not limited to online data protection. The APPI was significantly amended in 2015 and the amendment took effect on May 30, 2017.[2] The major aspects of the amendments are as follows:

- "Personal information" was newly defined, for clarification
- Small-business operators handling five thousand or fewer items of personal information became subject to the APPI
- "Sensitive personal information" was defined and must be treated more carefully

[1] Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Act No. 57 of 2003 (May 30, 2003), *last amended by* Act No. 51 of 2016, English translation as amended by Act No. 65 of 2015 *available at* http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=2781, *archived at* https://perma.cc/SD3Z-UU8T.

[2] Act to Amend APPI and Other Acts, Act No. 65 of 2015, Sup. Provisions art. 1; Order to Set the Enforcement Date of the Act to Amend the APPI and the Act on the Utilization of Personal Identification Numbers for Administrative Procedures, Order No. 385 of 2016.

- Rules for utilization of de-identified information were established
- Rules were established for cases where personal data is transferred to a third party in a foreign state
- The Personal Information Protection Commission (PIPC) was established
- Criminal penalties for the improper use of databases containing personal information for wrongful gain were created[3]

The Act on the Prohibition of Unauthorized Computer Access punishes a person who accesses a computer by circumventing access control measures.[4]

In addition, the Act on the Protection of Personal Information Held by Administrative Organs[5] and the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.[6] apply to the handling of personal information by government agencies and independent administrative agencies. These two laws are not discussed in this report.

B. Personal Information

The APPI defines the term "personal information" to mean information about a living person that identifies that person by name, date of birth, or other description, including information that will allow easy reference to other information and will thereby enable the identification of the person.[7] Personal information also includes personally identifiable signs, such as fingerprint data and the identification numbers of various documents.[8]

During the discussion of the 2015 amendments to the PPI, the discussion group established by the government[9] considered whether data about customer behaviors, such as the history of

---

[3] PIPC, OUTLINE OF THE AMENDED PERSONAL INFORMATION PROTECTION ACT (Feb. 2016), https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf, *archived at* https://perma.cc/B2DQ-AE2C.

[4] Fusei akusesu kōi no kinshi ni kansuru hōritsu [Act on the Prohibition of Unauthorized Computer Access], Act No. 128 of 1999 (Aug. 13, 1999), *amended by* Act No. 28 of 2013, art. 2, para. 4 & art. 3, English translation *available at* http://www.japaneselawtranslation.go.jp/law/detail/?id=2250&vm=02&re=02&new=1, *archived at* https://perma.cc/2UBQ-WEYM.

[5] Gyōsei kikan no hoyū suru kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information Held by Administrative Organs] (APPIHAO), Act No. 58 of 2003 (May 30, 2003), *last amended by* Act No. 51 of 2016, English translation as amended by Act No. 102 of 2005 *available at* http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=131, *archived at* https://perma.cc/9MEE-536A.

[6] Dokuritsu gyōsei hōjin tō no hoyū suru kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information Held by Independent Administrative Agencies], Act No. 59 of 2003 (May 30, 2003), *last amended by* Act No. 94 of 2011 (Aug. 10, 2011).

[7] APPI art.2, para. 1.

[8] Kojin jōhō no hogo ni kansuru hōritsu shikōrei [Enforcement Order of the Act on the Protection of Personal Information (APPI Order)], Order No. 507 of 2003, *amended by* Order No. 324 of 2016, art. 1.

[9] *Discussion Meeting on Personal Data*, PERSONAL DATA COMMISSION, IT STRATEGIC HEADQUARTERS, https://www.kantei.go.jp/jp/singi/it2/pd/index.html (last visited Nov. 20, 2017), *archived at* https://perma.cc/JD4A-VL3U.

smartphone application downloads and the history of access to various websites, should be covered as personal information under the APPI. These data do not directly identify a person, but data subjects can be identified by referring other personal data to such data. Because the government decided not to expand the definition of personal information with the 2015 amendment, information that itself does not identify a person, including customer behavior data, was excluded from the coverage of personal information under the APPI.[10]

C. Right to Privacy

There is a no legal provision that explicitly protects the right to privacy; however, the right to privacy has been recognized by the courts. The scope of personal information protected under the APPI is different from the scope of the right to privacy, though they overlap. Aspects of online privacy that are not covered by the APPI appear to be covered by the right to privacy as defined by the courts.

The first Supreme Court decision recognizing the right to privacy was rendered in 1969.[11] The Court stated that individuals have the right not to have their photos taken without consent.[12] In 2003 decision, the Supreme Court stated that information concerning a student's name, phone number, address, student number, and his/her application to attend a lecture is not in and of itself confidential information, but his/her expectation that such information would not be disclosed without reason should be protected. Therefore, this information is subject to legal protection as a right concerning privacy.[13] In 2017, the Supreme Court, citing its 2003 decision, stated that information concerning a person's minor child's name, sex, date of birth, address, phone number and his/her (parents') names is subject to legal protection as information involving privacy.[14]

D. Government's Roles

The government has established the Basic Policy on the Protection of Personal Information,[15] as required by the APPI.[16] The Basic Policy sets out the basic direction and actions to be taken by

---

[10] Katsuya Uga, 個人情報保護法の逐条解説 [Article by Article Commentaries on PIPA] at 41 (2016), https://lccn.loc.gov/2017407262.

[11] S. Ct., 1965 (A) No. 1187, 23 KEISHŪ 12, 1625 (Dec. 24, 1969), http://www.courts.go.jp/hanrei/ pdf/js_2010 0319120221050991.pdf, *archived at* https://perma.cc/ZEP8-TN8B, English-language summary of decision available on Courts of Japan website, *at* http://www.courts.go.jp/english/judgments/text/1969.12.24-1965.-A-.No..1187.html, *archived at* https://perma.cc/EG65-8TJL.

[12] S. Ct., 1965 (A) No. 1187.

[13] S. Ct., 2002 (Ju) No. 1656, 57 Minshu 8, 973 (Sept. 12, 2003), http://www.courts.go.jp/app/files/hanrei_jp/357/ 052357_hanrei.pdf, *archived at* https://perma.cc/TKE4-TT7M.

[14] S. Ct., 2016 (Ju) No. 1892 (Oct. 23, 2017), http://www.courts.go.jp/app/files/hanrei_jp/154/087154_hanrei.pdf, *archived at* https://perma.cc/P568-8ECE.

[15] Kojin jōhō no hogo ni kansuru kihon hōshin [Basic Policy on the Protection of Personal Information], Cabinet Decision (Apr. 2, 2004), *last amended by* Cabinet Decision (Oct. 28, 2016), https://www.ppc.go.jp/files/pdf/ 290530_personal_basicpolicy.pdf, *archived at* https://perma.cc/PE8A-8LC8.

[16] APPI art. 7.

the state, local public bodies, independent administrative agencies, and entities handling personal information.

Under the APPI, the Personal Information Protection Commission (PIPC) was placed under the jurisdiction of the Cabinet Office in order to oversee the handling of personal information by businesses.[17] The PIPC can require business operators handling personal information to submit reports and materials, and PIPC employees can visit businesses in order to interview their staff and inspect business records.[18] The PIPC can delegate this authority to the government ministers who have jurisdiction over the area of business of the relevant business operators.[19]

The PIPC can provide advice to businesses handling personal information.[20] When such a business neglects its legal obligations, the PIPC may recommend that the business operator cease the violation(s) and take other necessary corrective measures. If the business does not take the recommended measures without justifiable grounds, and when the PIPC finds that a serious infringement of the rights and interests of individuals is imminent, the PIPC may order the business operator to take the recommended measures.[21] Business operators that do not follow such orders may be punished by imprisonment for not more than six months or a fine of not more than 300,000 yen (approximately US$2,700).[22]

II. Protection of Personal Information Under the APPI

A. Businesses Handling Personal Information

The APPI applies to any business operators in Japan that hold personal data.[23] A business operator that handles personal information must take necessary and proper measures to prevent the leakage, loss, or damage of the data.[24] However, when the press, academic institutions, religious organizations, and political organizations deal with personal information for a specified purpose, such as broadcasting, research, religious or political activities, they are excluded from the APPI requirements. Instead, they must seek to take necessary and appropriate measures for controlling the security of personal data, and necessary measures for processing complaints about the handling of personal information, and make such measures public.[25]

---

[17] *Id*. arts. 59 & 60.

[18] *Id*. art. 40.

[19] *Id*. art. 44. If the matter relates to employment management, the Minister of Health, Labor and Welfare will have jurisdiction. *Id*. art. 46.

[20] *Id*. art. 41.

[21] *Id*. art. 42.

[22] *Id*. art. 84.

[23] *Id.* art. 2, para. 5. Note that Item 5 of article 2, paragraph 5 (Small-business exemption) was repealed by the 2015 amendment.

[24] *Id*. art. 20.

[25] *Id*. art. 76.

B. Purpose of Utilization and Requirement for Consent

The APPI requires business operators handling personal information to specify the purpose for which personal information is utilized as much as possible.[26] Upon acquiring personal information, a business must promptly notify the data subject of the purpose of its utilization, unless it has otherwise publicly announced the purpose.[27] Businesses must not use deception or other wrongful means to acquire personal information.[28]

When businesses acquire sensitive personal information that may trigger discrimination or other disadvantages, such as information related to race, religion, social status, health records, criminal records, and a history of being a crime victim,[29] they must obtain the consent of the data subject, unless

- acquiring the information is based on laws and regulations;
- acquiring the information is necessary for the protection of the body or property of an individual and it is difficult to obtain the consent of the data subject;
- acquiring the information is especially necessary for public health or promoting the sound growth of children and it is difficult to obtain the consent of the data subject;
- acquiring the information is necessary in order for the business to cooperate with national government agencies, local governments, or persons who were entrusted by these to conduct activities that are prescribed by law and obtaining prior consent is likely to impede execution of the work;
- the information has been made public by the government or institutions specified by the Commission; or
- acquiring the personal information is otherwise allowed by a Cabinet Order.[30]

A business also must obtain consent from data subjects before using the information for any other purpose than the one originally notified.[31] However, prior consent may not be necessary when the handling of personal information is

- based on laws and regulations necessary for the protection of life;
- necessary to protect the body or property of an individual and it is difficult to obtain the consent of the data subject;

[26] *Id*. art. 15, para. 1.

[27] *Id*. art. 18, para. 1.

[28] *Id*. art. 17, para. 1.

[29] *Id*. art. 2, para. 3.

[30] *Id*. art. 17, para. 2.

[31] *Id*. art. 16, para. 1.

- especially necessary for public health or promoting the sound growth of children and it is difficult to obtain the consent of the data subject; or
- necessary in order for the businesses to cooperate with national government agencies, local governments, or persons who were entrusted by these to conduct activities that are prescribed by law and obtaining prior consent is likely to impede the execution of the work.[32]

A business handling personal information cannot change the purpose of its utilization to one that is not duly related to the original one.[33] When the purpose is changed, the data subjects must be notified of the new purpose.[34]

C. Disclosure to the Data Subject

With respect to retained personal data, a business operator handling personal information must make the following information readily available to data subjects:

- The name of the business operator
- The purpose of utilization of all retained personal data
- The procedures for requesting corrections and disclosure, and for filing complaints[35]
- Contact information for the entity that accepts complaints[36]

When a data subject requests that a business operator disclose retained personal data that may lead to the identification of the person, the business operator must disclose the retained personal data to the person without delay. Such disclosure includes notifying the data subject that the business operator has no such retained personal data that may lead to his/her identification.[37] However, the business operator may keep all or part of the retained personal data undisclosed in cases where disclosure

- is likely to harm the life, body, property, or other rights or interests of the data subject or a third party;
- is likely to seriously impede the proper execution of the business of the business operator handling personal information; or
- violates other laws and regulations.[38]

---

[32] *Id*. art. 16, para. 3.

[33] *Id*. art. 15, para. 2.

[34] *Id*. art. 18, para. 3.

[35] *Id.* art. 27, para. 1.

[36] *Id*. and Enforcement Order of the APPI, art. 5.

[37] APPI art. 28.

[38] *Id*. art. 28, para. 2.

When a business operator has decided not to disclose all or part of such retained personal data, the business operator must notify the data subject of that decision and the underlying reason without delay.[39]

D. Transfer to a Third Party

A business operator handling personal information must not provide personal data to a third party without the prior consent of the data subject, except where the transfer is

- based on laws and regulations;
- necessary for the protection of the life, body, or property of an individual and it is difficult to obtain the consent of the data subject;
- especially necessary for improving public health or promoting the sound growth of children and it is difficult to obtain the consent of the data subject; or
- necessary for the affairs, prescribed by laws and regulations, conducted by a state organ, local government, or person who is authorized to conduct such affairs by these entities, where obtaining the consent of the person is likely to impede execution of the affairs.[40]

However, the data transfer is allowed if the business has notified the data subject about the following matters or made information regarding these matters easily available to the data subject:

- The fact that the data is to be transferred to the third party
- What information is to be transferred
- The method of transfer
- That the data subject can request to stop the transfer of information that can identify individuals
- The method for making such a request[41]

If the personal information is processed in such a way that individuals cannot be identified, such personally nonidentifiable information can be transferred to a third party after the business makes public the type of information to be transferred and method of the transfer.[42]

When businesses transfer personal information to a third party in a foreign country the prior consent of data subjects is, in principle, required. However, if the foreign country has a system to protect personal information that is considered to be of the same level as Japan, or the third

[39] *Id*. art. 28, para. 3 & art. 31.

[40] *Id*. art. 23, para. 1. One example of the final exception is when hospitals submit certain patient information to the national cancer survey.

[41] *Id*. art. 23, para. 2.

[42] *Id*. art. 36, para. 3 & art. 37.

party has a system to properly deal with personal information that meets the standards established by the PIPC, prior consent to the transfer to a foreign country is not required.[43] However, consent to transfer personal information to a third person is still needed.[44]

Businesses must keep records of transfers of personal information to third parties.[45] Recipients of such data from a third party must obtain the name (or representative's name in case of an entity) and address of the third party, and confirm the history of the data acquisition by the third party.[46]

E. Complaints and Requests to Businesses

The APPI states that a business operator must endeavor to establish a system for data subjects to complain about the handling of personal information and endeavor to appropriately and promptly process complaints.[47]

A data subject can request that a business operator correct, add, or delete personal data that may lead to the identification of the person when the personal data is contrary to the facts. The business operator must investigate the situation without delay and correct, add, or delete the retained personal data if it is found to be contrary to the facts, and inform the requester of the action taken.[48]

When a data subject finds that a business operator is using the retained personal data in a manner that may lead to the identification of the person beyond the stated purpose for the utilization of the data, or learns that the data was acquired improperly, he or she may request that the business operator discontinue using or erase such retained personal data.[49] Also, when a data subject finds that a business operator is providing retained personal data that may lead to the identification of the person to a third party without following the procedures stated above, he or she may request that the business operator discontinue the transfer.[50] When the business operator finds that the request is well-founded, it must discontinue using or erase the retained personal data concerned, or cease providing it to a third party, without delay.[51] However, if it would cost a large amount of money or would otherwise be difficult to discontinue using, erase, or discontinue the transfer of the data, the business operator may take alternative measures as

---

[43] *Id*. art. 24.

[44] YASUTAKA TSUJIBATA, Q&A DE WAKARI YASUKU MANABU HEISEI 27NEN KAISEI KOJIN JOHO HOGOHO [EASILY STUDYING PERSONAL INFORMATION PROTECTION ACT AMENDED IN 2015 BY Q&A], at 72 (2016).

[45] APPI art. 25.

[46] *Id*. art. 28, para. 1.

[47] *Id*. art. 35.

[48] *Id*. art. 29.

[49] *Id*. art. 30, para. 1.

[50] *Id*. art. 30, para. 3.

[51] *Id*. art. 30, para. 2 & 4.

long as those measures can protect the rights and interests of the person.[52] The business operator must promptly notify the data subject of its decision and, when the request is declined, the reason for refusing to act.[53]

F. Certified Personal Information Protection Organization

Many business organizations issued guidelines on personal information protection and regulated their members before the enactment of the APPI.[54] Business organizations conduct the following activities for the purpose of ensuring the proper handling of personal information by their members:

- Processing complaints about the handling of personal information
- Providing information for business operators to ensure the proper handling of personal information
- Any other activities necessary for ensuring the proper handling of personal information by member entities[55]

Such organizations engaged in personal information protection activities may be certified by the PIPC.[56] A certified personal information protection organization must endeavor to issue guidelines concerning specifying the purpose of utilization of personal information, security control measures, procedures for complying with individuals' requests, methods to create information that do not identify individuals, and other matters.[57]

A data subject may file a complaint about the handling of personal information by a business operator with a personal information protection organization if the business operator is a member of the organization. When such an organization receives a complaint, it must give the data subject necessary advice and investigate the circumstances pertaining to the complaint. The organization also forwards the complaint to the business operator and requests that the operator resolve the complaint promptly.[58]

---

[52] *Id*.

[53] *Id*. art. 30, para. 5.

[54] SHIZUO FUJIWAYA AND KOJIN JŌHŌ HOGO HŌSEI KENKYŪKAI [PERSONAL INFORMATION LAW RESEARCH STUDY GROUP], KOJIN JŌHŌ HOGO HŌ NO KAISETSU [COMMENTARY ON THE ACT ON THE PROTECTION OF PERSONAL INFORMATION] 219 (Itsuo Sonobe ed., 2005).

[55] APPI art. 47, para. 1.

[56] *Id*. art. 47, para. 2. The list of Certified Personal Information Protection Organizations are available on PIPC's website, at https://www.ppc.go.jp/personal/nintei/list/ (last visited Nov. 16, 2017), *archived at* https://perma.cc/EQ7E-4PKK.

[57] APPI art. 53, para. 1. For example, the Japan Data Communications Association's guideline is available at http://www.dekyo.or.jp/kojinjyoho/law/1.html (in Japanese), *archived at* https://perma.cc/BF3R-BSBN.

[58] APPI art. 52, para. 1.

G. Criminal Penalty for Data Theft

When persons who handle or previously handled personal information provide third parties with personal information databases that were acquired in relation to their business, or use those databases for the purpose of seeking illegal profits for themselves or third parties, they are subject upon conviction to imprisonment for not more than one year or a fine of not more than 500,000 yen (approximately US$4,500).[59]

III. Unauthorized Access to Computers

The Act on the Prohibition of Unauthorized Computer Access punishes a person who accesses a computer by circumventing access control measures, such as using the authorized person's identification and password without authorization or by creating a security hole.[60] The following acts are also prohibited:

- Obtaining and storing another person's identification and password without authorization for the purpose of unauthorized computer access[61]
- Providing another person's identification and password without authorization to a third person who does not have authority to use them[62]

An act of unauthorized access is punishable by imprisonment for not more than three years or a fine of not more than one million yen (about US$9,000).[63] Other acts listed above are punishable by imprisonment of not more than one year or a fine of not more than 500,000 yen (about US$4,500).[64]

IV. Right to Be Forgotten

In a case involving a petitioner who claimed his right to privacy was violated by Google because reports of his arrest for child prostitution in 2011 were shown in Google searches, the court of first instance, the Saitama District Court, recognized the man's "right to be forgotten" and ordered Google to delete the search results.[65] However, the Tokyo High Court reversed the decision and did not recognize the right to be forgotten. The High Court stated that the right to be forgotten did not have to be independently considered, because it was not yet a concrete concept, and it could be included in the discussion of the right to privacy and defamation.[66] The

---

[59] *Id*. art. 83.

[60] Act on the Prohibition of Unauthorized Computer Access, Act No. 128 of 1999 (Aug. 13, 1999), *amended by* Act No. 28 of 2013, art. 2, para. 4 & art. 3.

[61] *Id*. arts. 4 & 6.

[62] *Id*. art. 5.

[63] *Id*. art. 11.

[64] *Id*. art. 12.

[65] Saitama Dist. Ct., (Dec. 22, 2015), HANREI JIHO 2282, 78.

[66] Tokyo High Ct. (July 12, 2016), HANREI TAIMUZU 1429, 112 (Dec. 2016).

Supreme Court did not mention the right to be forgotten when it affirmed the High Court's decision on January 31, 2017.[67]

The Supreme Court recognized that the petitioner had a right to privacy, but found that the provision of Internet search results had the character of an act of expression by Google, because the search program reflects Google's policies on internet searches. The Court held that Google has the right to freedom of expression. In addition, the Court recognized in general the importance of internet search engines like Google's in society.[68]

The Court set forth the general rule that the adverse effects of invasion of privacy versus the importance of the provision of search results must be weighed in individual cases, and when the right to privacy prevails, the person whose information was revealed can demand the deletion of the search results. The Court set forth the elements to be considered in balancing the two, including the

- nature of the information,
- extent to which the information is spread by the search results,
- extent of adverse effects for the person who is the subject of the search,
- public status of the searched person, and
- purpose and meaning of the presentation of the information on the websites.[69]

V. PrivacyMark

The Japan Information Processing Development Corporation (JIPDEC) established the "PrivacyMark" system in 1998 upon instruction from the Ministry of International Trade and Industry (currently the Ministry of Economy, Trade and Industry, or METI).[70] This system assesses whether a business operator has taken appropriate measures to protect personal information and grants those who meet certain standards the right to display the PrivacyMark label in the course of their business activities.[71] The system provides incentives for business operators to gain social credibility. A PrivacyMark conformity assessment body evaluates the business operator's compliance with all relevant laws and regulations.[72] The system is in compliance with Japan Industrial Standards (Personal Information Protection Management

[67] Heisei 28 (Kyo) 45 (S. Ct., Jan. 31, 2017), http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482 (click Chinese characters beside the PDF icon), *archived at* https://perma.cc/4RL2-JXMM & https://perma.cc/UU8T-AP2K.

[68] *Id*.

[69] *Id*.

[70] *About the Privacy Mark: Outline and Objective*, JIPDEC, https://privacymark.org/about/outline_and_purpose.html (last modified Nov. 20, 2017), *archived at* https://perma.cc/5DWT-YGUB.

[71] *Id*.

[72] *Id*.

System – Requirements, JIS Q15001 (2006)). JIS Q15001 is in the process of being amended. The standards for PrivacyMark will be amended after the amended JIS Q15001 is published.[73]

In accordance with the PrivacyMark agreement, a business operator who obtains the right to use the mark must report any incidents in which data subjects' personal information was leaked. JIPDEC reviews the incidents and may cancel the grant of the right to use the PrivacyMark.[74]

[73] JIS改正に関連したプライバシーマーク付与適格性審査の対応方針について [*Regarding Eligibility Examination for PrivacyMark Corresponding to JIS Amendment*], JIPDEC, https://privacymark.jp/system/operation/jis_kaisei.html (last visited Nov. 21, 2017), *archived at* https://perma.cc/329F-Y72Y.

[74] 個人情報の取扱いに関する事故の報告について[*Reporting Accidents of Handling Personal Information*], JIPDEC, https://privacymark.jp/system/accident/index.html (last modified Nov. 21, 2007), *archived at* https://perma.cc/T27T-KF45.

EU Countries

European Union

Jenny Gesley
Foreign Law Specialist

SUMMARY Since 2012, the EU has implemented its proposed reform of the existing legislative framework on the protection of personal data and has published another proposal. The 2002 Directive on Privacy and Electronic Communications (ePrivacy Directive) and the General Data Protection Regulation (GDPR), which entered into force May 2016, currently form the two main pillars of the data protection legal framework in the EU. The GDPR replaced and updated the 1995 data protection rules with the goals of strengthening online privacy rights, boosting Europe's digital economy, and streamlining the implementation of data protection rules in EU Member States. In order to align the rules on electronic communications with technical developments and with the GDPR, the European Commission published a legislative proposal for a regulation on privacy and electronic communications on January 10, 2017. The proposed regulation would repeal and replace the 2002 ePrivacy Directive and take effect in May 2018.

I. Introduction

The protection of personal data and the respect for private life are fundamental rights in the European Union (EU).[1] Personal data is defined as "any information relating to an identified or identifiable natural person (data subject)."[2] Since publication of the Law Library of Congress's 2012 report on online privacy law, the EU has implemented the proposed reform of the existing legislative framework on the protection of personal data discussed in the report and in 2017 published another proposal. The data protection legal framework in the EU currently consists of two main pillars, the Directive on Privacy and Electronic Communications (ePrivacy Directive)[3] and the General Data Protection Regulation (GDPR).[4]

---

[1] Charter of Fundamental Rights of the European Union (EU Charter) arts. 7, 8, 2012 O.J. (C 326) 391, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN, *archived at* http://perma.cc/PJN3-A8MZ; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 16, para. 1, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, *archived at* http://perma.cc/K69X-SDQ9.

[2] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) art. 4 (1), 2016 O.J. (L 119) 1, http://eur-lex.europa eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH. An identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *Id.*

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (ePrivacy Directive), 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/legal-content /EN/TXT/PDF/?uri=CELEX:32002L0058&from=en, *archived at* http://perma.cc/LCQ4-LCJR.

[4] *See* GDPR, *supra* note 2.

The EU's first rules for the protection of personal data were adopted in 1995, when the internet was still in its infancy.[5] The 1995 Data Protection Directive set out general rules to safeguard the right to privacy with regard to the processing of personal data and provided for the free movement of such data in the Member States.[6] It stipulated that any processing of personal information required the explicit consent of the person concerned and that advance information about such data processing had to be provided to the data subject.[7] Since then, globalization and technological advancements have brought new challenges for the protection of personal data and required a reform of the EU data protection framework.

In January 2012, the European Commission presented a plan for a comprehensive reform of the EU's 1995 data protection rules. The goals of the reform were to strengthen online privacy rights, boost Europe's digital economy, and streamline the implementation of data protection rules in the EU Member States.[8] One of the concerns with the 1995 rules was that they had been implemented in differing ways in the Member States, leading to fragmentation.[9] The reform plan included a policy communication[10] setting out the Commission's objectives and two legislative proposals—one for a General Data Protection Regulation (GDPR)[11] and one for a Criminal Law Enforcement Data Protection Directive.[12] The GDPR[13] and the Criminal Law Enforcement Data Protection Directive[14] were adopted in April 2016. The GDPR entered into force on May 24,

---

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN, *archived at* http://perma.cc/DW3S-KL29.

[6] *Id*. art. 1.

[7] *Id*. arts. 7, 10.

[8] European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.pdf, *archived at* http://perma.cc/BXE7-682P.

[9] *Id.*

[10] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM (2012) 9 final (Jan. 25, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en, *archived at* http://perma.cc/MT7A-X6NG.

[11] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN, *archived at* http://perma.cc/76TF-GZQS.

[12] *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN, *archived at* http://perma.cc/UZ96-M46T.

[13] *See* GDPR, *supra* note 2.

[14] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal penalties, and

2016, and will apply directly in the EU Member States beginning May 25, 2018.[15] The Criminal Law Enforcement Data Protection Directive entered into force on May 5, 2016.[16] The deadline for implementation into national law for EU Member States is May 6, 2018.[17]

On January 10, 2017, the European Commission published another legislative proposal that aims to align current rules with technical developments and with the GDPR. The proposed regulation on privacy and electronic communications (ePrivacy Regulation) would repeal the ePrivacy Directive 2002/58/EC[18] and particularize and complement the GDPR, meaning that all matters concerning the processing of personal data not specifically addressed in the proposal would be covered by the GDPR.[19] The proposed regulation would take effect on May 25, 2018.[20]

Other EU legislative instruments on personal data protection included Directive 2006/24/EC on data retention.[21] However, Directive 2006/24/EC was declared invalid by the Court of Justice of the European Union (ECJ) on April 8, 2014, because it violated the right to privacy (article 7), the right to protection of personal data (article 8), and the principle of proportionality (article 52) as codified in the EU Charter.[22] It has not been replaced with new EU legislation. Instead, national data retention laws are applicable, but they are subject to review by the ECJ.[23] The ECJ held that data retention obligations and access to that data are only permissible under EU law if they are strictly necessary.[24] In the Court's opinion, EU law precludes national legislation that

---

on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Criminal Law Enforcement Data Protection Directive), 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN, *archived at* http://perma.cc/X8TW-3C9Z.

[15] GDPR, *supra* note 2, art. 99.

[16] Criminal Law Enforcement Data Protection Directive, *supra* note 14, art. 64.

[17] *Id*. art. 63.

[18] ePrivacy Directive, *supra* note 3.

[19] *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (ePrivacy Regulation)*, COM(2017) 10 final (Jan. 10, 2017), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, *archived at* http://perma.cc/YX4Q-G2KX.

[20] *Id*. art. 29, para. 2.

[21] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=EN, *archived at* http://perma.cc/AG3E-MEPT.

[22] Joined Cases C-293/12 and C-594/12, Dig. Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/XZK2-Y7D5. For background information, see THERESA PAPADEMETRIOU, EUROPEAN UNION: ECJ INVALIDATES DATA RETENTION DIRECTIVE (Law Library of Congress, June 2014), http://www.loc.gov/ law/help/eu-data-retention-directive/eu-data-retention-directive.pdf, *archived at* http://perma.cc/B8VM-XTDU.

[23] Joined Cases C-203/15, Tele2 Sverige AB v. Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v. Tom Watson, paras. 75–81, ECLI:EU:C:2016:970, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 62015CJ0203, *archived at* http://perma.cc/PT73-PD2J.

[24] *Id*. at 96.

prescribes general and indiscriminate retention of data.[25] The Commission has announced that it will develop guidance as to how national data retention laws can be constructed to comply with the ECJ ruling.[26]

II. Legal Framework

A. General Data Protection Regulation

The GDPR builds upon the 1995 Data Protection Directive and updates and modernizes the principles enshrined in it to deal with the challenges posed by the digital economy. In order to avoid the fragmentation that resulted from the differing implementation and enforcement of the 1995 directive in the EU Member States, the Commission opted for a regulation. The regulation will be directly applicable in the Member States with generally no domestic implementing legislation needed.[27]

1. Material and Territorial Scope

According to section 2 of the GDPR, the regulation applies to the "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data."[28]

The territorial scope covers businesses with an EU establishment where personal data is processed "in the context of the activities" of that establishment. It is irrelevant whether the data processing itself takes place in the EU.[29] "Establishment" is broadly defined by the ECJ. It held that the "concept of 'establishment' . . . extends to any real and effective activity—even a minimal one—exercised through stable arrangements."[30] The presence of only one representative can, in some circumstances, suffice.[31]

---

[25] *Id.* at 112.

[26] *Communication from the Commission to the European Parliament, the European Council and the Council. Fourth Progress Report Towards an Effective and Genuine Security Union*, COM (2017) 041 final (Jan. 25, 2017), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0041&from=EN, *archived at* http://perma.cc/JTJ4-6P9T.

[27] TFEU, *supra* note 1, art. 288, para. 2; GDPR, *supra* note 2, art. 99. Some provisions nonetheless require for their implementation the adoption of measures of application by the Member States—for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR. The GDPR also contains "opening clauses" that permit diverging national legislation in certain areas—for example, for the processing of special categories of personal data or in the context of employment.

[28] GDPR, *supra* note 2, art. 4(2).

[29] *Id*. art. 3, para. 1.

[30] Case C-230/14, Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság, paras. 30, 31, ECLI:EU:C:2015:639, http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0230&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/7HF3-BGJR; GDPR, *supra* note 2, recital 22.

[31] *Id*.

If the organization has no establishment in the EU, the GDPR applies where the processing activities are related to the offering of goods and services to data subjects located in the EU or where the behavior of EU data subjects is monitored.[32] Monitoring behavior includes, in particular, tracking an EU resident on the internet as well as the potential subsequent use of personal data processing techniques to profile that person—for example to analyze or predict her or his personal preferences, behaviors, and attitudes.[33]

Lastly, the GDPR will apply to organizations without an EU establishment if the law of a Member State applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post.[34]

2. *Principles Relating to Processing of Personal Data*

Personal data may only be processed if certain principles are complied with. These principles are

> (a) lawfulness, fairness, and transparency;
> (b) purpose limitation, meaning personal data may only be collected for specified, explicit, and legitimate purposes and not be further processed in a manner that is incompatible with those purposes;
> (c) data minimization, meaning processing of personal data should be adequate, relevant, and limited to what is necessary;
> (d) accuracy and keeping data up to date;
> (f) storage limitation, meaning that personal data in a form which permits identification of data subjects may not be kept longer than is necessary for the purposes for which the personal data are processed; and
> (g) integrity and confidentiality to ensure the appropriate security of the processed personal data.[35]

The controller processing the data is responsible for compliance with the aforementioned principles and has to be able to demonstrate such compliance.[36]

[32] GDPR, *supra* note 2, art. 3, para. 2.

[33] *Id.* recital 24.

[34] *Id.* art. 3, para. 3; recital 25.

[35] *Id.* art. 5, para. 1.

[36] *Id.* art. 5, para. 2.

a. Lawfulness in General

Article 6 of the GDPR sets out the conditions under which the data processing is considered lawful. The most common ground is consent given by the data subject.[37] Other grounds include when the data processing is necessary for

- performance of a contract with the data subject or to take steps preparatory to such a contract;[38]
- compliance with a legal obligation;[39]
- protection of the vital interests of a data subject or another person where the data subject is incapable of giving consent;[40]
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;[41] or
- legitimate interests pursued by the controller or by a third party.[42]

b. Consent

Consent is only valid if it is freely given,[43] specific, informed,[44] and an unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of personal data relating to him or her.[45] It may be withdrawn at any time.[46] Silence, pre-ticked boxes, or inactivity do not constitute consent.[47] In addition, consent is not valid in the context of a contract including the provision of a service, if the data subject is required to give consent to uses of his or her personal data that are not necessary for the performance of the contract or service.[48] There is a presumption that such consent is not freely given.[49] When the processing has multiple purposes, separate consent must be given to each for all of them to be valid.[50]

---

[37] *Id.* art. 6, para. 1(a), art. 7.

[38] *Id.* art. 6, para. 1(b).

[39] *Id.* art. 6, para. 1(c); art. 6, para. 3; recitals 41, 45.

[40] *Id.* art. 6, para. 1(d); recital 46.

[41] *Id.* art. 6, para. 1(e); art. 6, para. 3; recital 45.

[42] *Id.* art. 6, para. 1(f); recitals 47–50.

[43] *Id.* art. 7, para. 4; recital 43.

[44] *Id.* recital 42.

[45] *Id.* art. 4(11).

[46] *Id.* art. 7, para. 3.

[47] *Id.* recital 32.

[48] *Id.* art. 7, para. 4; recital 43.

[49] *Id.*

[50] *Id.* recital 32.

When "information society services"[51] are offered directly to children, consent is subject to specific rules.[52] If the child is younger than sixteen years, parental consent is needed for the processing to be lawful. Member States may lower the age to thirteen. Because children are regarded as particularly vulnerable, any information or communication to a child has to be easily understandable in clear and plain language.[53]

c. Fairness and Transparency

In order to ensure fairness and transparency, data controllers must provide data subjects with extensive information, unless they already have this information, at the time the data is obtained.[54] The information includes, among other things, the controller's identity and contact details, the data protection officer's contact details, the purposes and the legal basis of the data processing, the "legitimate interests" pursued by the controller or by a third party if this is used as a legal basis, personal data recipients or recipient categories, details of data transfers outside the EU if applicable, the retention period, rights of the data subject to his or her data, and the possibility of submitting a complaint to a supervisory authority.[55]

d. Sensitive Personal Data

In general, processing sensitive personal data is prohibited.[56] Sensitive data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or a natural person's sex life or sexual orientation. The processing of photographs is only considered processing of biometric data if it allows the unique identification or authentication of a natural person.[57] As an exception, sensitive data may be processed if the data subject has given explicit consent for one or more specified purposes or if one of the other enumerated grounds allows the processing, including obligations under a collective agreement or under employment, social security, or social protection law.[58] The GDPR

[51] "Information society services" are defined as services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. *See* Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services art. 1, para. 1(b), 2015 O.J. (L 241) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN, *archived at* http://perma.cc/HS39-U8Z3. Annex I provides an indicative list of services that are not covered by the term.

[52] GDPR, *supra* note 2, art. 8.

[53] *Id.* art. 12, para. 1; recital 58.

[54] *Id.* arts. 12–14.

[55] *Id.* art. 13.

[56] *Id.* art. 9, para. 1.

[57] *Id.* recital 51.

[58] *Id.* art. 9, para. 2.

allows Member States to maintain or adopt further conditions, including limitations, with regard to the processing of genetic, biometric, or health data.[59]

3. *Rights of Data Subjects*

The GDPR grants data subjects various rights with respect to their data. Among them are the right of information and access,[60] the right to data portability,[61] the right to rectification,[62] the right to erasure ("right to be forgotten"),[63] the right to restriction,[64] and several rights to object to data processing. After a data subject makes a request based on these rights, action must generally be taken without undue delay and, in any event, within one month of receipt of the request.[65]

a. Right of Information and Access

The right of information and access provides the data subject with the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, when that is the case, access to the personal data and supplemental information.[66] The controller must provide a copy of the processed data to the data subject free of charge.[67] If the request is made electronically, the information should be provided in a commonly used electronic form.[68]

b. Right to Data Portability

The right to data portability is broader than the right to receive data in a commonly used electronic form, but it only applies to personal data that the data subject has provided to the controller, that was processed under consent or contract, and that is processed by automated means. It requires the controller to provide information to the data subject in a structured, commonly used, and machine-readable form. The data subject can also require the controller to transmit those data to another controller.[69]

---

[59] *Id.* art. 9, para. 4.

[60] *Id.* art. 15.

[61] *Id.* art. 20.

[62] *Id.* art. 16.

[63] *Id.* art. 17.

[64] *Id.* art. 18.

[65] *Id.* art. 12, para. 3.

[66] *Id*. art. 15.

[67] *Id.* art. 15, para. 3.

[68] *Id*.

[69] *Id.* art. 20.

c. Right to Rectification

The right to rectification gives the data subject a right to require the controller to rectify inaccurate personal data concerning him or her and in some cases to complete incomplete information.[70]

d. Right to Be Forgotten

The right to erasure ("right to be forgotten") provides data subjects with the right to require controllers to erase personal data when certain conditions are met.[71] The provision draws from a May 13, 2014, decision by the ECJ.[72] A data subject may demand erasure if

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing on the basis of legitimate interests and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed in breach of the GDPR;
- the personal data must be erased to comply with an EU or Member State legal obligation to which the controller is subject; or
- the personal data have been collected in relation to the offer of information society services directly to a child and consent was given by the child, but he or she was not fully aware of the risks involved by the processing at the time, and later wants to remove such personal data.[73]

If one of these grounds for erasure applies and the controller has made the personal data public, he or she has to take reasonable steps to inform other controllers who are processing the data that the data subject has requested erasure of any links to, or copies or replications of, those personal data.[74] The right to erasure may be restricted if an exemption applies, such as if the processing is necessary to exercise freedom of expression and information.[75]

---

[70] *Id.* art. 16.

[71] *Id.* art. 17.

[72] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T. For a summary of the case, *see* Theresa Papademetriou, *Court of Justice of the European Union: Decision Upholds Right to Have Personal Data Erased*, GLOBAL LEGAL MONITOR (May 21, 2014), http://www.loc.gov/law/foreign-news/article/court-of-justice-of-the-european-union-decision-upholds-right-to-have-personal-data-erased/, *archived at* https://perma.cc/Q36W-JCB9.

[73] GDPR, *supra* note 2, art. 17, para. 1; recital 65.

[74] *Id.* art. 17, para. 2; recital 66.

[75] *Id.* art. 17, para. 3.

e. Right to Restriction

Instead of erasure, the data subject may have a right to restriction of processing of personal data. Restriction means that the controller may only store the data but not process it further.[76] A right to restriction exists if

- the accuracy of the personal data is contested by the data subject while the controller verifies it;
- the processing is unlawful and the data subject requests the restriction instead of erasure;
- the controller no longer needs the personal data for processing purposes, but the data subject requires them for the establishment, exercise, or defense of legal claims; or
- the data subject has objected to processing based on legitimate interests pending the verification of whether the controller has overriding legitimate grounds.[77]

f. Rights to Object to Processing

Data subjects have several rights to object to the processing of personal data carried out for specific purposes.[78] They have an absolute right to object at any time where personal data are processed for direct marketing purposes.[79] If the processing is necessary for the performance of a task carried out in the public interest, or if it is necessary for legitimate interests pursued by the controller,[80] the data subject may object to the processing on grounds relating to his or her particular situation.[81] If the processing is done for scientific or historical research purposes or statistical purposes, the data subject has a right to object on grounds relating to his or her particular situation, unless the processing is necessary for the performance of a task carried out in the public interest.[82]

4. Supervision

The GDPR states that its provisions will be enforced by an independent national supervisory authority in each Member State.[83] In cases where the processing of personal data takes place in more than one Member State (cross-border processing), the business will be primarily regulated by the supervisory authority in the Member State in which it has its main establishment (the lead supervisory authority).[84] The lead supervisory authority must cooperate with the national

[76] *Id.* art. 18, para. 2.

[77] *Id.* art. 17, para. 1.

[78] *Id.* art. 21; recitals 69, 70.

[79] *Id.* art. 21, para. 2.

[80] *Id.* art. 6, paras. 1(e), (f).

[81] *Id.* art. 21, para. 1.

[82] *Id.* art. 21, para. 6.

[83] *Id.* arts. 51, 52.

[84] *Id.* arts. 56, 60.

supervisory authorities in the other Member States where the business is established, and they may conduct joint operations.[85] The approach adopted in the final version of the regulation is a watered-down version of the initial proposal. The proposal envisaged a "one-stop shop" under which a business conducting cross-border processing would only have to deal with a single supervisory authority to ensure a uniform application.[86] This proposal was not adopted because Member States were opposed to the idea.

In addition, the GDPR creates an independent European Data Protection Board (EDPB) with legal personality.[87] The EDPB is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. It monitors the application of the GDPR and advises the EU Commission, issues guidelines, recommendations, and best practices on particular issues, and adjudicates disputes arising from supervisory authority decisions.[88]

5. Notification of Data Breach and Penalties

If there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, the data controller has an obligation to notify the supervisory authority and the data subject without undue delay if the breach is likely to result in a high risk to the rights and freedoms of natural persons.[89] Failure to provide notification of a breach may result in administrative fines of up to €10 million (about US$10.9 million), or in the case of an undertaking, of up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[90]

6. Remedies for Data Subjects

Data subjects have the right to lodge a complaint with their supervisory authority against data processors and controllers if the processing of personal data infringes the GDPR.[91] If there has been an infringement, data subjects have a right to receive compensation for damages from the processor or controller.[92] The GDPR provides that the concept of damages "should be broadly interpreted in the light of the case law of the Court of Justice in a manner which fully reflects the objectives of this Regulation."[93] Furthermore, the GDPR authorizes not-for-profit bodies,

---

[85] *Id.* arts. 60–62.

[86] COM (2012) 11 final, *supra* note 11, para. 3.4.6.2.; recitals 97, 98; art. 51, para. 2.

[87] GDPR, *supra* note 2, arts. 68, 69.

[88] *Id.* arts. 65, 70.

[89] *Id.* arts. 4(12), 33, 34.

[90] *Id.* art. 83, para. 4.

[91] *Id.* art. 77.

[92] *Id.* art. 82.

[93] *Id.* recital 146.

organizations, or associations to lodge complaints on behalf of data subjects with supervisory authorities.[94]

B. The ePrivacy Directive

Currently, rules on privacy and electronic communications are codified in the ePrivacy Directive 2002/58/EC[95] as modified by the Cookies Directive.[96] It was adopted in 2002 and states, among other things, how the principles in the 1995 Data Protection Directive apply to the electronic communications sector.[97] The proposed regulation on electronic privacy mentioned above would repeal and replace the directive.[98]

The aim of the ePrivacy Directive is to ensure an equivalent level of protection of fundamental rights and freedoms (particularly the right to privacy) with respect to personal data processing in the electronic communications sector and to ensure the free movement of such data.[99] The ePrivacy Directive covers processing of personal data by traditional telecom providers in public communications networks in the EU and mandates that Member States protect the confidentiality of the content of electronic communications through national legislation.[100]

With regard to cookies and other identifiers, the ePrivacy Directive requires Member States to ensure that storing or gaining access to information already stored in a subscriber or user's terminal equipment is only allowed if the subscriber or user concerned has given his or her consent.[101]

Traffic data, defined as "any data processed for the purpose of a conveyance of a communication on an electronic communications network or for the billing thereof,"[102] must be deleted or made anonymous when it is no longer needed. Exceptions are allowed for billing purposes and national security reasons, among others.[103]

---

[94] *Id.* art. 80.

[95] *See* Directive 2002/58/EC, *supra* note 18.

[96] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement on Consumer Protection Laws (Cookies Directive), 2009 O.J. (L 337) 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, *archived at* http://perma.cc/KW92-SUVC.

[97] ePrivacy Directive, *supra* note 3, art. 1, para. 2.

[98] *See* COM(2017) 10 final, *supra* note 19.

[99] ePrivacy Directive, *supra* note 3, art. 1, para. 1.

[100] *Id.* arts. 3, 5.

[101] *Id.* art. 5, para. 3.

[102] *Id.* art. 2(b).

[103] *Id.* art. 6; art. 15, para. 1.

Location data, defined as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service,"[104] may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added service.[105] Value-added services are commonly known as location-based services. The provision is only applicable to electronic communications service providers and not to information society service providers.[106]

Article 13, paragraph 1 of the ePrivacy Directive contains rules with regard to unsolicited direct marketing. It prohibits the use of automated calling machines and the use of fax and email for direct marketing ("spam") without the prior consent of the subscriber or user. In 2004, the Article 29 Working Party, which was set up under article 29 of the 1995 Data Protection Directive as an independent European advisory body on data protection and privacy, concluded in an opinion that the prohibition applies exclusively to "messages by electronic communications" and not to messages exchanged via information society services.[107]

C. Proposal for an ePrivacy Regulation

The proposed regulation will enter into force after it has been adopted by both the European Parliament and the Council in what was formerly called the "co-decision procedure," now referred to as the ordinary legislative procedure.[108] Unlike the directive, it will be directly applicable in all EU Member States with no domestic implementing legislation needed.[109] In order to ensure uniform application in all Member States, the proposal provides that the regulation will be enforced by the independent national supervisory authorities already competent to enforce the GDPR.[110]

1. Content

The proposed ePrivacy Regulation would have a wider scope than the current directive. It would cover providing e-communications services to end-users in the EU, irrespective of whether the end-user is required to pay for the service; the use of such services; and the protection of information related to the terminal equipment of end-users located in the EU.[111] Providers that are located outside the EU would have to appoint a representative in the EU.[112]

---

[104] *Id.* art. 2(c).

[105] *Id.* art. 9, para. 1.

[106] For a definition of "information society services," see *supra* note 50.

[107] Article 29 Working Party, *Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC*, 11601/EN, WP 90 (Feb. 27, 2004), at 4, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf, *archived at* http://perma.cc/D4TG-PTVG.

[108] TFEU, *supra* note 1, arts. 289, 294.

[109] *Id*. art. 288, para. 2.

[110] ePrivacy Regulation, consideration 38, art. 18.

[111] *Id*. art. 3, para. 1.

[112] *Id*. art. 3, para. 2.

In addition to traditional telecom providers and the content of electronic communications, the proposed regulation would extend coverage to internet-based voice and messaging services such as WhatsApp, Facebook Messenger, and Skype.[113] The confidentiality of content and metadata derived from electronic communications would also be protected.[114]

The proposal aims to simplify the rules on consent for the use of tracking cookies and other identifiers. It suggests that browser settings or other applications should offer an easy way for an end user to allow or refuse cookies. It would be up to the user to opt for a lower or higher level of security (data protection by design).[115] No consent would be needed for non-privacy-intrusive cookies, such as those used to remember the content of an online shopping cart or to measure visitor traffic to a website.[116]

Furthermore, the ePrivacy Regulation would ban unsolicited spam marketing messages and calls received via email, SMS, and automated calling machines, irrespective of the technology used to convey these unsolicited communications.[117] However, the use of email contact details within the context of an existing customer relationship for the offering of similar products or services would be allowed. The email from the marketing company would be required to contain clear information on how to object to such a use.[118] The ePrivacy Regulation would also require marketing companies to either display their phone numbers or use a special code or prefix that indicates a marketing call.[119] In addition, it would require telecom providers to offer end users the means to limit the reception of unwanted calls and to block calls from specific numbers or from anonymous sources free of charge.[120]

2. Status of Negotiations

As mentioned, both the European Parliament and the Council have to adopt the regulation. Within the European Parliament, the proposal is assigned to the Civil Liberties Committee (LIBE) which issued a draft report on June 21, 2017.[121] More than eight hundred amendments

---

[113] *Id.* art. 18.

[114] *Id*. art. 4, no. 3a; art. 5.

[115] *Id.* recital 22.

[116] *Id*. arts. 8, 10.

[117] *Id*. art. 16.

[118] *Id*. art. 16, para. 2.

[119] *Id.* art. 16, para. 3.

[120] *Id*. art. 14.

[121] LIBE, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, doc. no. 2017/0003(COD), June 9, 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-606.011+01+DOC+PDF+V0//EN&language=EN, *archived at* http://perma.cc/D4A4-AFL2.

were submitted by the July 2017 deadline.[122] LIBE adopted the report on October 19, 2017, and presented it for a first reading of the plenary of the EU Parliament on October 23, 2017.[123]

Within the Council, the proposal was assigned to the Telecommunications and Information Society working party, which is in the process of discussing the proposal.[124] As several issues still need to be discussed, Member States' delegations have voiced concerns as to whether the proposed date of May 25, 2018, for the entry into force of the regulation can be achieved.[125]

[122] Jennifer Baker, *LIBE Submits More than 800 Amendments to ePrivacy Regulation*, IAPP (July 20, 2017), https://iapp.org/news/a/libe-submits-more-than-800-amendments-to-eprivacy-regulation/, *archived at* http://perma.cc/KNR7-BK7J.

[123] LIBE, *Report on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, doc. no. A8-0324/2017, Oct. 20, 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0324+0+DOC+PDF+V0//EN, *archived at* http://perma.cc/CMN6-LE3T.

[124] Council of the EU, General Secretariat, Notice of Meeting and Provisional Agenda, doc. no. CM 4609/17, Oct. 19, 2017, http://data.consilium.europa.eu/doc/document/CM-4609-2017-INIT/en/pdf, *archived at* http://perma.cc/4RL2-2ATA.

[125] European Parliament, *Legislative Train Schedule: Proposal for a Regulation on Privacy and Electronic Communications* (last updated Oct. 20, 2017), http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-e-privacy-reform, *archived at* http://perma.cc/4R3G-9STC.

France

Nicolas Boring
Foreign Law Specialist

A significant development with respect to online privacy law in France since 2012 is the October 2016 adoption of the Law for a Digital Republic.[1] The majority of this Law's provisions have to do with issues such as ensuring internet neutrality, developing a knowledge economy, and increasing the public's access to the digital world.[2] However, this Law also includes several provisions on the subject of online privacy.[3]

Specifically, the Law for a Digital Republic strengthened the powers of the Commission Nationale de l'Informatique et des Libertés (National Commission on Computer Technology and Civil Liberties, CNIL), mainly by increasing the maximum sanction that it can impose on a website owner for failure to comply with a demand to remove private information, from €150,000 (approximately US$176,260) to €3 million (approximately US$1.18 million).[4] The Law for a Digital Republic also amended the French Penal Code to prohibit the unauthorized dissemination of sexually-explicit recordings (so-called "revenge porn").[5] Such acts are now punishable by up to two years in jail and/or a fine of up to €60,000 (approximately US$70,500).[6]

The 2016 Law also introduced the concept of a "digital last will and testament" into French law: a person may now give instructions regarding the communication, retention, or deletion of online data concerning that person after his/her death.[7] Additionally, the Law introduced a "right to be forgotten" that is specific to minors, with an accelerated procedure for the exercise of that right.[8] Any person may request that his/her personal information be removed from a website or

---

[1] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique [Law No. 2016-1321 of 7 October 2016 for a Digital Republic], https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8C156142EB5E2B6314C1CCE69972F229.tplgfr31s_2?cidTexte=JORFTEXT000033202746&categorieLien=id, *archived at* https://perma.cc/V4K6-2AHX.

[2] *Id.*

[3] *Id.* arts. 54–68.

[4] *Id.* art. 65; *République numérique: que change la loi du 7 octobre 2016 ?* [*Digital Republic: What Does the Law of 7 October 2016 Change?*], VIE-PUBLIQUE.FR (French government website) (Oct. 19, 2016), http://www.vie-publique.fr/actualite/dossier/loi-internet/republique-numerique-que-change-loi-du-7-octobre-2016.html, *archived at* https://perma.cc/SW5F-KZQY.

[5] Loi n° 2016-1321 du 7 octobre 2016, art. 67.

[6] *Id.*

[7] *Id.* art. 63; *Ce que change la loi pour une République numérique pour la protection des données personnelles* [*What is Changed by the Law for a Digital Republic for the Protection of Personal Data*], CNIL (Nov. 17, 2016), https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles, *archived at* https://perma.cc/J4TP-8DVC.

[8] Loi n° 2016-1321 du 7 octobre 2016, art. 63; *Ce que change la loi pour une République numérique pour la protection des données personnelles*, CNIL, *supra* note 7.

database, but whereas the organization in charge of the website or database has two months to reply when the requester is an adult,[9] it must do so within one month if the requester is a minor.[10]

[9] *Le droit d'opposition* [*The Right to Opposition*], CNIL, https://www.cnil.fr/fr/le-droit-dopposition (last visited Nov. 7, 2017), *archived at* https://perma.cc/NFY3-GJED.

[10] Loi n° 2016-1321 du 7 octobre 2016, art. 63; *Ce que change la loi pour une République numérique pour la protection des données personnelles*, CNIL, *supra* note 7.

Germany

Jenny Gesley
Foreign Law Specialist

SUMMARY Since 2012, several online data privacy reforms have been initiated or implemented in Germany. Whether or not the European Union Cookie Directive from 2009 has been properly implemented in Germany is subject to disagreement. In 2015, Germany passed a new Data Retention Act and the data retention obligations were supposed to apply to telecommunications providers starting on July 1, 2017. However, following a preliminary court decision that raised doubts about the compatibility of the German Act with EU law, the German Federal Network Agency decided to suspend the obligation for all providers until a final decision. Starting on May 25, 2018, the European Union General Data Protection Regulation will apply directly in Germany. It is supplemented by provisions of the amended German Data Protection Act.

Since 2012, several online data privacy reforms have been initiated or implemented in Germany, as further discussed below.

I. EU Cookie Directive

European Union (EU) Directive 2009/136/EC on the processing of personal data and the protection of privacy in the electronic communications sector (the Cookie Directive),[1] which amended the ePrivacy Directive,[2] has still not been expressly implemented in Germany. The amendment deals with the use of cookies and similar techniques, and the consent of the user as a requirement for storing or gaining access to information.[3] The German government claims that an implementation is not necessary as existing German law already conformed to the requirements of the Cookie Directive[4] and the EU Commission initially seemed to share that

[1] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement on Consumer Protection Laws (Cookie Directive), 2009 O.J. (L 337) 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, *archived at* http://perma.cc/KW92-SUVC.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (ePrivacy Directive), 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en, *archived at* http://perma.cc/LCQ4-LCJR.

[3] Cookie Directive art. 5, para. 3.

[4] European Commission, Directorate-General for the Information Society and Media, *Questionnaire on the Implementation of the Article 5(3) of the ePrivacy Directive* 7 (Oct. 4, 2011), https://www.telemedicus.info/uploads/Dokumente/COCOM11-20QuestionnaireonArt.53e-PrivacyDir.pdf, *archived at* http://perma.cc/N6SV-CMA4.

view.[5] However, a study prepared for the EU Commission in 2015 noted that Germany had not transposed the amendment of the ePrivacy Directive.[6] German federal and state data protection authorities are of the view that the German rules do not completely implement the amended EU Directive.[7] In any case, the proposed EU ePrivacy Regulation,[8] which will replace the ePrivacy Directive, contains new rules on cookies, so that the discussion of whether or not the EU Directive has been properly implemented will become obsolete when the Regulation enters into force, which is proposed to occur on May 25, 2018.

II. Data Retention

EU Directive 2006/24/EC on data retention was declared invalid by the Court of Justice of the European Union (ECJ) on April 8, 2014, and has not been replaced by new EU legislation.[9] Instead, national data retention laws are applicable, but they are subject to review by the ECJ.[10] In December 2015, Germany passed a new Data Retention Act, which amended the German Telecommunications Act (TCA) and the German Code of Criminal Procedure.[11] The amended provisions of the TCA obligate providers of publicly available telecommunication services to store certain user traffic data for a period of four weeks (location data) or ten weeks

---

[5] Adrian Schneider, *EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt* [*EU Commission: Cookie Directive has Been Implemented in Germany*], TELEMEDICUS (Feb. 5, 2014), https://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html, *archived at* http://perma.cc/T7NB-T39V.

[6] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY AND MEDIA, EPRIVACY DIRECTIVE: ASSESSMENT OF TRANSPOSITION, EFFECTIVENESS AND COMPATIBILITY WITH PROPOSED DATA PROTECTION REGULATION. FINAL REPORT 63 (Jan. 31, 2015), https://publications.europa.eu/en/publication-detail/-/publication/573b8f74-7220-41d7-9e4b-477ab1d45e29, *archived at* http://perma.cc/5SZ6-KQGW.

[7] Düsseldorfer Kreis, Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015. Keine Cookies ohne Einwilligung der Internetnutzer [Decision of the Data Protection Commissioners of the Federation and the States of February 5, 2015. No Cookies Without Consent of the Internet User], https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/Entschliessungen_zwischen_den_Konferenzen/20150205_Keine_Cookies_ohne_Einwilligung_der_Internetnutzer/Keine_Cookies_ohne_Einwilligung_der_Internetnutzer1.pdf, *archived at* http://perma.cc/9K2N-EYJB.

[8] *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (ePrivacy Regulation)*, COM (2017) 10 final (Jan. 10, 2017), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, *archived at* http://perma.cc/YX4Q-G2KX.

[9] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/XZK2-Y7D5.

[10] Joined Cases C-203/15, Tele2 Sverige AB v. Post-och telestyrelsen & C-698/15 Sec'y of State for the Home Dep't v. Watson, paras. 75–81, ECLI:EU:C:2016:970, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 62015CJ0203, *archived at* http://perma.cc/PT73-PD2J.

[11] Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten [Act Introducing a Storage Obligation and a Maximum Retention Period for Traffic Data], Dec. 10, 2015, BUNDESGESETZBLATT [BGBL.] [FEDERAL LAW GAZETTE] I at 2218, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf, *archived at* http://perma.cc/8PF2-7P9K, English translation of draft act *available at* http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2015&num=288&dLang=EN, *archived at* http://perma.cc/X7R8-W9WN.

(communication data) and make them available to law enforcement upon request.[12] User metadata that need to be retained by internet access service providers include IP addresses, port numbers, and the date and time of internet access.[13] The amendments entered into force in December 2015 and the data retention obligations were supposed to apply to the providers after an interim period starting on July 1, 2017.[14] However, on June 22, 2017, the Higher Administrative Court of North Rhine-Westphalia held in an application for an interim order that the plaintiff in the case, a telecommunications provider, need not comply with the data retention obligation until the court has reached a final judgment.[15] The Court stated that it was doubtful whether the German data retention provisions were compatible with the requirements for national data retention laws as formulated by the ECJ.[16]

Even though the judgment only has effect for the parties involved in the case, the German Federal Network Agency (Bundesnetzagentur), a higher federal authority that regulates the telecommunications sector, decided to suspend the data retention obligations of the TCA for all providers until the final judgment and thus will not levy any fines for failure to comply until then.[17] Separately, the Parliamentary Research Services of the German Parliament has also found that the German data retention provisions are incompatible with the requirements for data retention that the ECJ formulated in its judgment.[18]

---

[12] Telekommunikationsgesetz [TKG] [Telecommunications Act] [TCA], June 22, 2004, BGBL. I at 1190, as amended, §§ 113a-113g, http://www.gesetze-im-internet.de/tkg_2004/TKG.pdf, *archived at* http://perma.cc/BJ7H-RVHL.

[13] *Id*. § 113b, para. 3.

[14] *Id*. § 150, para. 13.

[15] Oberverwaltungsgericht NRW [Higher Administrative Court of NRW], June 22, 2017, docket no. 13 B 238/17, http://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2017/13_B_238_17_Beschluss_20170622.html, *archived at* http://perma.cc/AD9C-U67C.

[16] Joined Cases C-203/15, Tele2 Sverige AB v. Post-och telestyrelsen & C-698/15 Sec'y of State for the Home Dep't v. Watson, paras. 75–81, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 62015CJ0203, *archived at* http://perma.cc/PT73-PD2J.

[17] Bundesnetzagentur [Federal Network Agency], Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten [Storage Obligation and a Maximum Retention Period for Traffic Data], June 28, 2017, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html;jsessionid=399D3A7061786CA903F0173F0D900C7F?nn=329286#Inhalt, *archived at* http://perma.cc/73CZ-G3M8.

[18] WISSENSCHAFTLICHE DIENSTE [PARLIAMENTARY RESEARCH SERVICES], ZUR VEREINBARKEIT DES GESETZES ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN MIT DEM EUGH-URTEIL VOM 21. DEZEMBER 2016 ZUR VORRATSDATENSPEICHERUNG [ON THE COMPATIBILITY OF THE ACT INTRODUCING A STORAGE OBLIGATION AND A MAXIMUM RETENTION PERIOD FOR TRAFFIC DATA WITH THE JUDGMENT OF THE ECJ OF DECEMBER 21, 2016 ON DATA RETENTION] 24, doc. no. PE 6 – 3000 – 167/16, Jan. 12, 2017, https://www.bundestag.de/blob/492116/d7f0beffe3ae7b37bd666d6b70e2cd22/pe-6-167-16-pdf-data.pdf, *archived at* http://perma.cc/Z6ER-RLH8.

III. General Data Protection Regulation

The EU General Data Protection Regulation (GDPR)[19] entered into force on May 24, 2016, and will apply directly in Germany starting on May 25, 2018, with generally no domestic implementing legislation needed.[20] However, the GDPR also contains "opening clauses" that permit derogations for national legislation in certain areas[21] and specifically allows EU Member States to incorporate elements of the GDPR into their national law as far as necessary for coherence and making it comprehensible.[22] Germany therefore published the amendment of its Data Protection Act, which aligns it with the requirements of the GDPR and the EU Law Enforcement Directive (EU) 2016/680, in July 2017—the first EU Member State to do so.[23] It will enter into force at the same time as the GDPR will apply in Germany, on May 25, 2018.[24]

The new German Data Protection Act focuses on the areas for which the GDPR contained "opening clauses" allowing Member States to initiate more restrictive provisions, as the other areas are governed by the provisions of the GDPR itself. It also has a wider scope than the GDPR; it applies to the processing of personal data by federal and state public authorities and bodies as well as by private bodies.[25] The new German Data Protection Act took advantage of the opening clauses related to collection and use of employee data,[26] special categories of data (sensitive data),[27] processing of data for research purposes and statistical purposes,[28] processing

---

[19] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) art. 4 (1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

[20] *Id*. art. 99; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 288, para. 2, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, *archived at* https://perma.cc/K69X-SDQ9. Some provisions nonetheless require for their implementation the adoption of application measures by the Member States—for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR.

[21] GDPR, *supra* note 19, recitals 10, 19, 52; art. 9, para. 4; art. 88.

[22] *Id.* recital 8.

[23] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) [Act to Adapt the Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Data Protection Adaption and Implementation Act EU)], June 30, 2017, BGBL. I at 2097, http://www.bgbl.de/xaver/bgbl/start.xav?startbk= Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf, *archived at* http://perma.cc/DL3C-LKGD, English translation *available at* https://www.bmi.bund.de/SharedDocs/downloads/EN/gesetztestexte/datenschutzanpassungs umsetzungsgesetz.pdf?__blob=publicationFile&v=1, *archived at* http://perma.cc/K79T-PMUW.

[24] *Id*. art. 8.

[25] *Id*. art. 1, § 1; GDPR, *supra* note 19, recital 19.

[26] Data Protection Adaption and Implementation Act EU, art. 1, § 26.

[27] *Id.* art. 1, § 22.

[28] *Id.* art. 1, § 27.

for archiving purposes in the public interest,[29] processing for other purposes than the ones for which the personal data have been originally collected,[30] restrictions on the investigative power of data protection authorities in cases of professional secrecy,[31] appointment of data protection officers,[32] consumer loans,[33] credit reports and scoring,[34] sanctions,[35] the right of data protection authorities to file an action against a decision of the EU Commission,[36] video surveillance,[37] and restrictions on some of the data subjects' rights.[38]

With regard to online privacy rights, the restrictions on the data subject's right to erasure and to access data are the most important differences compared to the GDPR. If in a case of nonautomated data processing erasure is impossible or only possible with a disproportionate effort due to the specific mode of storage, and if the data subject's interest in erasure is minimal, the right to erasure is replaced with a right to restriction of processing as codified in article 18 of the GDPR. This modification is not applicable if the processing was unlawful. Furthermore, the right to restriction applies instead of the right to erasure if erasure would conflict with a legal duty of the controller to retain the data for a specific time period.[39]

The Act restricts the right to access personal data in cases where they are only stored because the data may not be deleted due to legal provisions mandating retention (archived data), or the personal data are solely kept for purposes of monitoring or safeguarding data, or for data protection audits, and providing information would require a disproportionate effort.[40]

Lastly, the German Data Protection Act requires each company with ten or more employees involved in the automated processing of personal data to appoint a data protection officer, whereas the GDPR only obligates public authorities or bodies and entities whose core activities consist of processing operations that require regular and systematic monitoring of data subjects or processing of special categories of data on a large scale to appoint one.[41]

---

[29] *Id.* art. 1, § 28.

[30] *Id.* art. 1, § 24.

[31] *Id.* art. 1, § 29, para. 3.

[32] *Id.* art. 1, § 38.

[33] *Id.* art. 1, § 30.

[34] *Id.* art. 1, § 31.

[35] *Id*. art. 1, §§ 41 et seq.

[36] *Id*. art. 7, no. 5, § 42b.

[37] *Id*. art. 1, § 4.

[38] *Id*. art. 1, §§ 32–37.

[39] *Id.* § 35, para. 3; GDPR, *supra* note 19, art. 17, para. 3b.

[40] Data Protection Adaption and Implementation Act EU, art. 1, § 34.

[41] *Id.* art. 1, § 31, GDPR, *supra* note 19, art. 37.

Italy

Dante Figueroa
Senior Legal Information Analyst

Italy has enacted a number of laws regulating online privacy in the country.[1] Since 2012, one minor provision regarding online privacy has been enacted in the context of a broad transparency law known as Legislative Decree No. 33 of 2013.[2]

Article 53 of Legislative Decree No. 33 repealed a provision of the 2003 Code on the Protection of Personal Data,[3] as amended, that provided certain protections for public employees, which stated as follows:

> Art. 19, ¶ 3-bis (Principles Applicable to the Treatment of Data other than Sensitive and Judicial Data): The respective administrative agency must make accessible notices concerning the performance of services of anyone who is in charge of a public function and the evaluation thereof. However, that obligation only applies in the cases established in the law, with respect to notices related to the nature of the illness or the personal or family impediments that cause absence from work, as well as referring to the components of the evaluation or notices regarding the employment relationship between the employee and the respective government agency, that have the capacity to reveal some of the information mentioned in article 4, ¶ 1(d) [regarding sensitive data].[4]

The repeal by Legislative Decree No. 33 means that an administrative agency may now legally reveal information about a public employee regarding the cause of an absence from work, or

---

[1] *Italian Legislation*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI [ITALIAN DATA PROTECTION AUTHORITY], http://www.garanteprivacy.it/web/guest/home_en/italian-legislation (last visited Dec. 7, 2017), *archived at* https://perma.cc/S7N7-YRP5.

[2] Decreto legislativo 14 marzo 2013, n. 33. Riordino della Disciplina Riguardante gli Obblighi di Pubblicità, Trasparenza e Diffusione di Informazioni da parte delle Pubbliche Amministrazioni [Legislative Decree No. 33 of March 14, 2013, concerning the Topic of the Obligations of Publicity, Transparency, and Dissemination of Information by Public Agencies] art. 53, GAZZETTA UFFICIALE [G.U.], No. 80 (Apr. 5, 2013), http://www.garanteprivacy.it/ web/guest/home/docweb/-/docweb-display/docweb/2576657, *archived at* https://perma.cc/5W7E-ZHXV.

[3] Decreto Legislativo 30 giugno 2003, n. 196, Codice in Materia di Protezione dei Dati Personali [Legislative Decree No. 196 of June 30, 2003, Code on the Protection of Personal Data] art. 19, ¶ 3-bis, G.U., No. 174 (July 29, 2003), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig=, *archived at* https://perma.cc/D42M-TLUF.

[4] Legge 4 novembre 2010, n. 183 Deleghe al Governo in materia di Lavori Usuranti, di Riorganizzazione di Enti, di Congedi, Aspettative e Permessi, di Ammortizzatori Sociali, di Servizi per l'Impiego, di Incentivi all'Occupazione, di Apprendistato, di Occupazione Femminile, nonche' Misure contro il Lavoro Sommerso e Disposizioni in Tema di Lavoro Pubblico e di Controversie di Lavoro [Law No. 183, of November 4, 2010, Delegation into the Government on Strenuous Work, Reorganization of Entities, Leave, Expectations and Permits, Social Safety Nets, Employment Services, Employment Incentives, Apprenticeship, Female Employment, as well as Measures against Submerged Work, and Provisions on Public Employment and Labor Conflicts] art. 14(1)(b) (adding ¶ 3-bis to art. 19 of the Code on the Protection of Personal Data), G.U., No. 262 (Nov. 11, 2010), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2010-11-04;183!vig, *archived at* https://perma.cc/FGD4-SWJA (translation by author).

other “sensitive data,” such as the employee’s race, ethnic origin, religion, political opinion, membership in a political party, union, or other organization, or personal data regarding health or sexual activity.

Netherlands

Wendy Zeldin
Senior Legal Research Analyst

SUMMARY Over the last five years, the Dutch parliament has adopted a number of amendments to laws that govern the privacy of online personal data. The Constitution was changed to protect privacy of telecommunications and the key law on personal data protection, the Personal Data Protection Act, underwent a significant overhaul in 2015 that enhanced breach notification procedures, increased fines for violation of the Act, and strengthened the powers of the newly titled Personal Data Authority. At the same time, changes were made to the Telecommunications Act, among them the addition of a new article setting forth the conditions on the permissibility of storage of or access to information in peripheral equipment of a user via an electronic communications network. In late 2015, the Authority issued rules to clarify what constitutes a data breach and the breach notification procedures. Earlier in 2015, following a decision reached in 2014 by the Court of Justice of the European Union, a Dutch judge struck down the 2009 Data Retention Act on grounds that it was too intrusive and breached the privacy of telephone and internet users. In 2017, the Dutch Senate adopted a new Act on Intelligence and Security Services. Some of the Act's provisions have entered into force, but on November 1 the Dutch Electoral Council announced that a referendum will be held within six months on the new Act. Among new developments that affect personal data privacy in the Netherlands are the 2017 legal certification of the government to use digital ledgers in the healthcare sector and the adoption of legislation that allows storage for up to four weeks of vehicle registration data recorded by automatic plate number recognition cameras set up at certain locations on public roads.

According to legal researchers at the Institute of eLaw at Leiden University, in a study comparing "aspects of privacy, such as government policy, legislation and monitoring and enforcement, in eight European countries," the Netherlands leads the other states in reporting requirements on data leaks, and the Dutch "have a high level of awareness and self-reliance with regard to their privacy." [1] The Netherlands is also reportedly one of the leaders in conducting societal debate and information campaigns on privacy, and in carrying out privacy impact assessments, which are "instruments for determining privacy risks of data processing in advance."[2] The study found, however, that in all the countries studied "transparency with regard to the collection and processing of personal data still leaves much to be desired," and the Netherlands has room to improve in such areas as the number of privacy officials, the certification of personal data security, and dialogue engaged in by the key privacy supervisory body, the Personal Data Authority.[3] Nevertheless, the researchers stated that "[t]he Dutch

[1] *The Netherlands One of the Leaders in Privacy Protection*, LEIDEN UNIVERSITY (Oct. 4, 2017), https://www.universiteitleiden.nl/en/news/2017/09/the-netherlands-one-of-the-leaders-in-privacy-protection, *archived at* https://perma.cc/QH4Z-TKH3.

[2] *Id.*

[3] *Id*.

government has already put many instruments into place relating to all aspects of the protection of privacy," and therefore "the country is well prepared for the General Data Protection Regulation (GDPR) to be implemented by the EU in May 2018."[4]

This report summarizes some of the major legal developments that have occurred in the area of online privacy law in the Netherlands over the last five years, since 2012.

I. Constitution

In 2012, the Staten-Generaal (States-General, the Dutch parliament) discussed amending article 13 of the Dutch Constitution,[5] on protection of privacy of correspondence, with a view to protecting communications more broadly. The parliament finally adopted the amendment in July 2017 and it was published in the *Official Gazette* in August, but is not yet in force.[6] The unamended article 13 states

> 1. The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.
> 2. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.[7]

The amended article states

> 1. Everyone is entitled to the right of privacy of correspondence and of telecommunications.
> 2. Limitation of this right may be determined in cases laid down by Act of Parliament, with the authorization of the court, or in the interests of national security, by or with the authorization of those designated for the purpose by Act of Parliament.[8]

---

[4] *Id.*

[5] CONSTITUTION OF THE KINGDOM OF THE NETHERLANDS (Aug. 24, 1815, as in force on Mar. 15, 2014), http://www.dutchcivillaw.com/legislation/constitution011.htm, *archived at* https://perma.cc/DE38-ETXH; Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815 (*as last amended* June 27, 2008, in force on July 15, 2008), http://wetten.overheid.nl/BWBR0001840/geldigheidsdatum_02-05-2012, *archived at* https://perma.cc/J879-68WP.

[6] Wet van 19 augustus 2017, houdende verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim [Law of 19 August 2017, Stating That There Are Grounds for Considering a Proposal to Amend the Constitutional Provision Concerning the Inviolability of Privacy of Correspondence and of Telephone and Telegraph Communications], STAATSBLAD VAN HET KONINKRIJK DER NEDERLANDEN [STB.] [OFFICIAL GAZETTE OF THE KINGDOM OF THE NETHERLANDS], No. 334 (Sept. 14, 2017), https://zoek.officielebekendmakingen.nl/stb-2017-334.html, *archived at* https://perma.cc/3LEL-YU7W.

[7] CONSTITUTION OF THE KINGDOM OF THE NETHERLANDS art. 13.

[8] Wet van 19 augustus 2017, art. 13.

II. Laws

A. Amendments to the Personal Data Protection Act

The Dutch Parliament passed a number of amendments to the Personal Data Protection Act (Wet bescherming persoonsgegevens, PDPA) [9] on May 26, 2015. Those amendments were published in June 2015, and came into force on January 1, 2016.[10] Among the key changes in the Act are the introduction of a general duty of notification of personal data breaches and a major increase in the fines that the renamed Data Protection Authority (College bescherming persoonsgegevens), now the Personal Data Authority (Autoriteit Persoonsgegevens, PDA), may impose for violations of the Act, along with enhanced PDA powers to fine individuals, such as directors, within an organization.[11] The changes "directly affect any company subject to Dutch law," thus companies were advised "to be aware of the new supervisory powers of the PDA and … to make the necessary amendments to their internal data protection and security policies. The latter particularly includes drafting or reviewing policies related to personal data breaches, as well as verifying that contracts with third parties adequately address these obligations."[12]

The adoption and entry into force of the amended Act preceded the EU's adoption of the GDPR on the protection of the processing of personal data and on such data's free movement.[13]

---

[9] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) [Law of 6 July 2000, Concerning Rules on the Protection of Personal Data (Personal Data Protection Act)] (*as last amended* effective July 1, 2017), http://wetten.overheid.nl/BWBR0011468/2017-07-01, *archived at* https://perma.cc/RZ4N-QP6K; Personal Data Protection Act [PDPA] (effective Jan. 1, 2016), https://www.akd.nl/t/Documents/17-03-2016_ENG_Wet-bescherming-persoonsgegevens.pdf, *archived at* https://perma.cc/2TQ3-AFHD; Berend van der Eijk, *Substantial Revision of the Dutch Data Protection Act: Higher Fines, Specific Obligations for Data Breaches and More*, BIRD & BIRD (June 23, 2015), *available at* https://www.lexology.com/library/detail.aspx?g=e16eb8af-f905-413f-93de-cd8675455c10, *archived at* https://perma.cc/D5P3-F22U.

[10] Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) [Act of 4 June 2015 Amending the Personal Data Protection Act and Any Other Laws in Connection with the Introduction of a Duty to Report in the Event of a Breach of Measures for the Security of Personal Data as well as the Extension of the Authority of the Data Protection Authority in Order to Comply with the Provisions of or to Impose an Administrative Fine Under or Pursuant to the Personal Data Protection Act (Duty to Report Data Leaks and Expansion of the Cbp Administrative Fine Power)] (Amendment Act of June 4, 2015), STB. No. 230 (June 19, 2015), https://zoek.officielebekendmakingen.nl/stb-2015-230.html, *archived at* https://perma.cc/SUD2-FL8Z.

[11] Van der Eijk, *supra* note 9.

[12] *Id.*

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1510677980976&uri=CELEX:32016R0679, *archived at* https://perma.cc/P684-DNSK.

1. Fines

Formerly, the PDA's capacity to impose fines was limited, and it could only impose an administrative fine of up to €4,500 (about US$5,300) for violation of the requirement to notify the PDA before commencing processing of personal data.[14] Moreover, while the agency could give an order to cease or remedy a violation of the Act, under threat of penalty, it could not impose an administrative fine.[15] Under the amended Act, the PDA may now impose fines up to €820,000 (about US$966,360) under the sixth category, the highest, of the latest fines schedule set forth in the Criminal Code,[16] or 10% of the entity's annual net turnover when a legal entity is involved and the highest category of fine is deemed insufficient punishment for the violation.[17] Increased fines of up to €20,500 (about US$24,160) are imposed on any non-EU entity that processes personal data in the Netherlands "without having designated a local representative to oversee compliance with the Dutch Data Protection Act."[18] Finally, the PDA may also impose separate fines of up to €820,000 on individuals within an organization, including directors and managers.[19]

2. Binding Orders

The amended PDPA provides that before the PDA may impose a fine, it must first issue a "binding order" (*een bindende aanwijzing*) after having conducted an investigation of an incidence of noncompliance with the Act.[20] As one commentator points out, "[t]his is a recovery-oriented corrective measure, in which the PDA specifies exactly what actions must be taken in order to remedy the non-compliance."[21] Moreover, the PDA "may set a time limit within which the offender must comply with the order," and if the offender fails to comply, the PDA may then apply the relevant punitive fine.[22] However, "if the violation was deliberate or the result of serious negligence" the PDA is not subject to the binding order requirement and may immediately impose the fine.[23]

---

[14] *Id.*; Part II(L), "Administrative and Criminal Sanctions," *in* WENDY ZELDIN, ONLINE PRIVACY LAW: NETHERLANDS (Law Library of Congress, June 2012), https://www.loc.gov/law/help/online-privacy-law/netherlands.php, *archived at* https://perma.cc/Y2JH-6N5E (with reference to art. 66 of the Act, imposing fines for violation of arts. 27, 28, and 79(1)).

[15] *Id.*

[16] PDPA art. 66; Wetboek van Strafrecht (Mar. 3, 1881, *as amended*) art. 23(4), http://wetten.overheid.nl/BWBR0001854/2017-09-01, *archived at* https://perma.cc/Q2ZG-LF9M.

[17] Van der Eijk, *supra* note 9; PDPA art. 66 ¶¶ 2 & 5; Wetboek van Strafrecht art. 23(7).

[18] Van der Eijk, *supra* note 9; PDPA art. 66(1) (with reference to arts. 4 & 78(2)).

[19] Van der Eijk, *supra* note 9; PDPA art. 66(2) (with reference, e.g., to art. 12(1): "Any person acting under the authority of the controller or of the processor, including the processor himself, in so far as they have access to personal data, only processes them on instructions from the controller, unless required to do so by law.").

[20] Van der Eijk, *supra* note 9; PDPA art. 66(3).

[21] Van der Eijk, *supra* note 9.

[22] PDPA art. 66(3).

[23] *Id.* art. 66(4); Van der Eijk, *supra* note 9.

A new article 67 in the Act accords the PDA the authority to issue a "policy rule" on the interpretation of article 66(2) on the imposition of fines of the highest category for violation of various provisions of the Act, provided that the PDA consults the Minister of Security and Justice and the Minister of the Interior and Kingdom Relations beforehand.[24] This will make it "easier for the PDA to construe 'wilful intent' or 'culpable negligence' in cases of non-compliance, allowing it to directly impose an administrative fine as described above."[25] He further comments that the consultation process "will generally also involve consultation with relevant industry stakeholders."[26]

3. New Article 34a on Data Breach Notification Obligation

Another major change made by the 2015 amendment to the Act was the introduction of a notification requirement for personal data breaches, without waiting for the issuance of the EU General Data Protection Regulation.[27] The notification duty under the Act "follows similar principles as seen across Europe and the rest of the world."[28] The new article 34a prescribes that a controller (*verantwoordelijke*, the responsible party), defined in the Act as "the natural or legal person or any other party who or the administrative body which, alone or jointly with others, determines the purposes and means of the processing of personal data,"[29] must notify the PDA without delay of any breach of personal data security that results in "a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data."[30]

Controllers must also immediately inform the individuals affected by the data breach, if the breach is likely to have a negative impact on the individual's privacy,[31] except in cases "where the controller has taken appropriate technical protective measures that render the personal data concerned incomprehensible or inaccessible to any person who does not have a right of access to the data."[32] Other exceptions to this duty to inform the affected individuals include, for example, where it is necessary in the interests of national security, the prevention of crime and the investigation and prosecution of criminal offenses, important economic or financial interests of the state and other public entities, monitoring compliance with the legal requirements established in connection with the interests of crime prevention/prosecution and economic/financial interests, and the protection of the data subject or of the rights and freedoms of others.[33] The new notification requirement also does not apply if the controller is a provider of a public

[24] PDPA art. 67; Van der Eijk, *supra* note 9.

[25] Van der Eijk, *supra* note 9.

[26] *Id*.

[27] *Id*. The GDPR, *supra* note 13, was adopted in 2016.

[28] Van der Eijk, *supra* note 9.

[29] PDPA art. 1(d).

[30] *Id*. art. 34a(1).

[31] *Id*. art. 34a(2).

[32] *Id*. art. 34a(6).

[33] *Id.* art. 43.

electronic communications service and has made a notification as such under the provisions of the Telecommunications Act.[34] The Telecommunications Act "has had a notification duty for security breaches with 'electronic communication providers' (such as telecom operators) for some time."[35] It prescribed that these providers had a duty to notify "any security breach which has an adverse effect on the privacy of individuals involved" to the telecom regulator (the Authority for Consumers and Markets, Autoriteit Consument en Markt) and individuals;[36] in conformity with the amended PDPA, the notifications must be addressed instead to the PDA.[37] Another exception to the duty to notify individuals of a breach is made for financial institutions "within the meaning of the Financial Supervision Act," e.g., banks and insurance companies,[38] "because a specific regulation for such institutions exists and includes a separate notification duty to the financial authority," the Autoriteit Financiële Markten (Dutch Authority for the Financial Markets, AFM).[39] One commentator noted that while financial institutions are obliged to report security breaches to the PDA and the AFM, and to keep a record of the breaches, "a duty for financial institutions to notify individuals of a breach is thought to have potential adverse and unexpected effects on the financial market, justifying the exemption to notify individuals."[40]

Under the new notification requirement, the notification of a breach made by controllers to the PDA and the persons concerned ("data subjects") must include "the nature of the breach, the bodies where more information about the breach can be obtained, and the measures recommended to limit the negative consequences of the breach."[41] The PDA notification must also provide "a description of the observed and probable consequences of the breach" and "the measures that the controller has taken or is proposing to take" in order to remedy them.[42] The data subject notification must be made in such a way as to guarantee, taking into account the nature of the infringement, the "proper and careful provision of the information" regarding the observed and actual consequences of the breach, the data subjects involved, and the costs of enforcement.[43] If the controller does not notify the data subject, the PDA may require the controller to do so if it deems the breach "likely to have unfavourable consequences for the data subject's privacy."[44]

---

[34] *Id*. art. 34a(9) (with reference to art. 11.3a, paras. 1 & 2, of the Telecommunications Act, Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet) (*as last amended* effective July 1, 2017), http://wetten.overheid.nl/BWBR0009950/2017-07-01, *archived at* https://perma.cc/C7M4-PA3Q).

[35] van der Eijk, *supra* note 9.

[36] *Id*.

[37] Telecommunicatiewet art. 11.3a(1).

[38] PDPA art. 34a(10); van der Eijk, *supra* note 9.

[39] van der Eijk, *supra* note 9.

[40] *Id*.

[41] PDPA art. 34a(3).

[42] *Id*. art. 34a(4).

[43] *Id*. art. 34a(5).

[44] *Id*. art. 34a(7).

4. New Language on Reporting Breaches

Controllers are obligated to keep a record of serious security breaches; the record is to include, in any case, "the facts and data regarding the nature of the breach … as well as the text of the notification to the data subject."[45] As noted by one commentator, "the new regime also obligates controllers to specifically address this requirement in their contracts with processors. Companies are therefore strongly advised to review their contractual relationship with their processors to ensure that this has been appropriately addressed."[46]

Thus, if a controller has a processor do the processing of personal data on the controller's behalf, the controller must ensure that the processor

> provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and in respect of the report of a breach of security, referred to in Section 13, which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data processed by him.[47]

Section 13 provides that the controller implements appropriate measures "to protect personal data against loss or any unlawful forms of processing" that "will guarantee a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" and "also seek to prevent the unnecessary collection and further processing of personal data."[48]

5. Enhanced Powers of Cooperation

Under a new article 51a of the PDPA, the PDA has gained enhanced powers "to share and request information from other supervisors, making it mandatory for supervisors to provide any information to other supervisors insofar as this is necessary for performing its supervisory tasks."[49] The article states as follows:

> 1. The Authority may make arrangements with other supervisory authorities in the interest of efficient and effective supervision of the processing of personal data and draw up cooperation protocols with these supervisory authorities for that purpose. Any cooperation protocol is to be published in the Government Gazette.
> 2. The Authority and the supervisory authorities, referred to in subsection 1, may on their own initiative and must on request disclose to one another the data relating to the processing of personal data that are necessary for the exercise of their functions.[50]

---

[45] *Id*. art. 34a(8).

[46] Van der Eijk, *supra* note 9.

[47] PDPA art. 14(1), *as amended by* Amendment Act of June 4, 2015, art. I(A).

[48] PDPA art. 13.

[49] Van der Eijk, *supra* note 9.

[50] PDPA art. 51a.

6. 2016 and 2017 Amendments to the PDPA

A few additional amendments to the PDPA were adopted in 2016 and 2017. Article 26 of the PDPA provides that orders in council (statutory regulation) may be issued in connection with the general rules on the processing of personal data governed under the PDPA's sections 6 through 11.[51] In October 2016 (effective July 2017), a new paragraph 3 was added to article 26 to the effect that presentation to the full legislature of an order in council in connection with the Act on the Use of a Citizen Service Number in Healthcare[52] can be done no sooner than four weeks after the draft order has been submitted to each Chamber of the States-General; if one of the Chambers decides not to approve the order, no presentation of it will be made and no new draft order will be presented to each Chamber sooner than six weeks after the decision of the disapproving Chamber has been made.[53]

In regard to healthcare data, on October 1, 2017, that the Dutch government had received "legal certification, the first of its kind in the healthcare sector" for "a digital ledger solution in the healthcare sector that would allow blockchain to be used for communications between the country's health institutions, including hospitals and government agencies."[54] Blockchain has been described as a digital "open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically."[55] The use of blockchain technology in the healthcare sector has four key advantages, according to one industry proponent: it "puts

---

[51] PDPA art. 26 para. 1.

[52] Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, i.e., Wet van 10 april 2008, houdende regels inzake het gebruik van het burgerservicenummer in de zorg (Wet gebruik burgerservicenummer in de zorg) [Act of 10 April 2008 Containing Rules Concerning the Use of the Citizen Service Number in Healthcare (Act on the Use of a Citizen Service Number in Healthcare)] (*as last amended* effective July 1, 2017), http://wetten.overheid.nl/BWBR0023864/2017-07-01, *archived at* https://perma.cc/KKX8-3FTD. According to this Act, "[r]ules may be laid down by or pursuant to an Order in Council on facts or data to be processed by care providers with regard to clients whose identification or citizen service number proves impossible, or requires a disproportionate effort, to find." *Id.* art. 11 para. 1. The Act further provides, "[b]y or pursuant to the Order in Council referred to in the first paragraph, it can be determined which security requirements the data processing referred to in the first paragraph meets." *Id.* art. 11 para. 2.

[53] PDPA art. 26 para. 3. Wet van 5 oktober 2016 tot wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens), STB. No. 373 (Oct. 19, 2016), https://zoek.officielebekendmakingen.nl/stb-2016-373.html, *archived at* https://perma.cc/5SN6-RWP2. Most provisions of the amendment entered into force on July 1, 2017. Besluit van 13 juni 2017, houdende vaststelling van het tijdstip van inwerkingtreding van de Wet van 5 oktober 2016 tot wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens) [Decree of 13 June 2017, Determining the Date of Entry into Force of the Law of 5 October 2016 Amending the Use of the Citizen Service Number in Healthcare, the Healthcare Market Organization Act, and the Health Insurance Act (Client Rights in Electronic Data Processing)], STB. 2016, No. 373, https://zoek.officielebekendmakingen.nl/stb-2017-279.html, *archived at* https://perma.cc/ZXW3-JA6X.

[54] Jennifer L. Schenker, *Dutch Government Gets Legal OK to Use Blockchain to Connect Healthcare Sector*, INNOVATOR (Oct. 1, [2017?]) https://innovator.news/dutch-government-gets-legal-ok-to-use-blockchain-to-connect-healthcare-sector-fb070ad0fa8d, *archived at* https://perma.cc/ZY7F-428R.

[55] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARVARD BUS. REV. (Jan.–Feb. 2017), https://hbr.org/2017/01/the-truth-about-blockchain, *archived at* https://perma.cc/S3X8-WT5G.

individuals in charge of their own data, allowing them to control which information will be released to a doctor or insurance company"; it connects scattered healthcare data "onto one digital highway, making it far more efficient"; it should result in a much lower cost of administering healthcare payments "because once a patient signals that he has used his digital wallet to pay for healthcare the insurance company is notified and a payment can be issued immediately"; and because transactions on the blockchain cannot be altered, "if someone wants to try and change the data they would have to break into six different data bases, making it … nearly impossible to hack."[56]

An amendment act of December 2016[57] changed several laws, including the PDPA, to conform to implementation of the 2014 EU Regulation on Electronic Identities and Trust Services.[58] The amending act added a new paragraph to PDPA article 34a on the data breach notification obligation, providing that the article, with one exception, does not apply to trust service providers as referred to in the EU Regulation.[59] A trust service provider is defined under the EU Regulation as "a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider."[60]

B. Telecommunications Act

In March 2015, an amendment to the Telecommunications Act, inserting a new article on the conditions in which storage of or access to information in the peripheral equipment of a user via an electronic communications network is permissible, was published in the *Official Gazette*. The article provides that, without prejudice to the PDPA, such storage or access is only permitted if the user concerned is (a) provided with clear and complete information in accordance with the PDPA, at least regarding the purposes for which this information is used; and (b) has given

---

[56] Schenker, *supra* note 54.

[57] Wet van 21 december 2016 tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) [Act of 21 December 2016 Amending the Telecommunications Act, Books 3 and 6 of the Civil Code, the General Administrative Law Act and Other Laws Relating to the Implementation of the EU Regulation on Electronic Identities and Trust Services (Implementation of EU Regulation on Electronic Identities and Trust Services)] (2016 Amendment Act), STB. No. 13 (Jan. 30, 2017), https://zoek.officielebekendmakingen.nl/stb-2017-13.html, *archived at* https://perma.cc/7763-RMTM.

[58] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG, *archived at* https://perma.cc/2KZS-AHRH.

[59] 2016 Amendment Act art. X, adding a new para. 10 to PDPA art. 34a.

[60] Regulation (EU) No. 910/2014, *supra* note 58, art. 3(19). A trust service is defined under art. 3(16) as follows:

> an electronic service normally provided for remuneration which consists of:
>
> (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
>
> (b) the creation, verification and validation of certificates for website authentication; or
>
> (c) the preservation of electronic signatures, seals or certificates related to those services; … .

permission for the storage or access.[61] These two requirements also apply in the event that, in a manner other than by means of an electronic communications network, information is stored via an electronic communications network or access is granted to information stored on the peripheral device.[62]

The provision on requirements for storage or access do not apply if the storage or access is (a) for the sole purpose of carrying out communication about an electronic communications network, or (b) strictly necessary in order to provide the information society service requested by the subscriber or user or, provided this has no or minor impact on the privacy of the subscriber or user concerned, to obtain information about the quality or effectiveness of a delivered information society service.[63] An activity that aims to collect, combine, or analyze data about the use by the user or subscriber of different services of the information society, so that the user or subscriber concerned "can be treated differently" (*anders behandeld kan worden*) is deemed to be a processing of personal data as referred to in article 1(b) of the PDPA.[64] User access to an information society service provided by or on behalf of a legal person set up under public law will not be made dependent on the granting of permission under the required conditions (a) and (b), above.[65] By or pursuant to an Order in Council, further rules may be laid down by the Minister of Security and Justice with regard to those conditions and the exceptions thereto (under art. 11.7a(3)). The Dutch Data Protection Authority is to be consulted on the draft of such an order.[66]

C. Data Breach Notification Rules

The Dutch Parliament heavily debated the notification obligation, along with the new supervisory powers of the PDA, because certain key aspects of the obligation needed more clarification, such as "what exactly qualifies as a breach? How to assess whether a breach is 'likely to have serious adverse consequences'? And what are 'negative effects to an individual's privacy'?"[67] The PDA issued guidelines to address these issues in December 2015.[68]

---

[61] Wet van 4 februari 2015 tot wijziging van de Telecommunicatiewet (wijziging artikel 11.7a) (in force on Mar. 10, 2015), art. 11.7a(1), https://zoek.officielebekendmakingen.nl/stb-2015-100.html, *archived at* https://perma.cc/P7PY-Z2MM.

[62] *Id.* art. 11.7a(2).

[63] *Id.* art. 11.7a(3).

[64] *Id.* art. 11.7a(4). PDPA art. 1(b) defines the processing of personal data as "any operation or set of operations which is/are performed upon personal data, including in any case the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data."

[65] Wet van 4 februari 2015 tot wijziging van de Telecommunicatiewet (wijziging artikel 11.7a), art. 11.7a(5).

[66] *Id.* art. 11.7a(6).

[67] Van der Eijk, *supra* note 9.

[68] Meldplicht datalekken Wet bescherming persoonsgegevens [Reporting Duty on Data Breaches under the Data Protection Act] (Rules) (in force on Dec. 16, 2015), http://wetten.overheid.nl/BWBR0037346/2015-12-16, *archived at* https://perma.cc/LA6G-UMVM (with Annex of articles cited from the PDPA).

The Reporting Duty on Data Breaches Under the PDPA Rules state, for example, that there is only a data breach if a security incident—e.g., loss of a USB stick, theft of a laptop, successful hacking attempts—has actually occurred, because not every security incident is also a data leak. A data breach exists if personal data has been lost during the security incident, or if the occurrence of unlawful processing of the personal data cannot reasonably be excluded; if there is only a weak spot in security, it is a "vulnerability," not a data breach, and does not have to be reported to the PDA.[69] Examples of personal data of a sensitive nature that should be reported to the DPA include

- special personal data as referred to in article 16 of the PDA, i.e., personal data about a person's religion or belief, race, political opinions, health, sexual life, membership in a trade union, and criminal personal data and personal data about unlawful or annoying behavior in connection with a prohibition imposed on that behavior;
- information about the financial or economic situation of the person concerned, such as data on (problematic) debts, salary, and payment data;
- data that can lead to stigmatization or exclusion of the person concerned (e.g., data on a gambling addiction, school or work performance, or relationship problems);
- user names, passwords, and other log-in details (depending on the possible consequences, such as the data to which the log-in details give access); [and]
- data that can be misused for (identity) fraud (e.g., biometric data, copies of identity documents, and the citizen service number).[70]

Other factors, such as the amount of personal data leaked per person or the number of data subjects whose personal data have been leaked, may also be grounds for reporting the data breach, but if the nature of the leaked data warrants it, the controller may have to report a data breach when the personal data of only one person are involved.[71]

The controller must report the breach "without undue delay and, if possible, no later than 72 hours after the discovery of the data breach."[72] The PDA website makes available on its website a web form for this purpose, through which the controller can supplement or withdraw the notification if necessary.[73] The Rules also cover such topics as notification of the person concerned, exceptions to the obligation to report, fines, a primer on the new reporting duty, and a schematic guide with key questions to consider in applying the new requirements.[74] The questions include, for example, "1. Does the duty to report data breaches from the Wbp apply to me?; 1.2. Am I the controller or his representative?," and so on. Under question 3.1, "Is there a

---

[69] *Id.*

[70] *Id.* The citizen service number (*burgerservicenummer*, BSN) "is a unique personal number allocated to everyone registered in the Personal Records Database (Basisregistratie Personen, BRP)." *Citizen Service Number (BSN)*, GOVERNMENT OF THE NETHERLANDS, https://www.government.nl/topics/personal-data/citizen-service-number-bsn (last visited Nov. 20, 2017), *archived at* https://perma.cc/TY8B-ETUW.

[71] Rules, *supra* note 68.

[72] *Id.*

[73] *Id.*

[74] *Id.*

breach of security?," the examples are "a lost USB stick; a stolen laptop; burglary by a hacker; a malware infection; and a calamity such as a fire in a data center."[75]
The Dutch guidelines were expected to stay close to the EU Article 29 Data Protection Working Party's opinion on personal data breach notification.[76]

D. 2017 Act on Intelligence and Security Services

The Dutch Senate adopted the new Act on Intelligence and Security Services (Wet op de inlichtingen- en veiligheidsdiensten, Wiv), in 172 articles, on July 26, 2017,[77] "after years of debate and criticism from both the country's constitutional courts and online privacy advocates."[78] The new Act is intended to replace the 2002 Act on Information and Security Services, laying down new rules on the duties and powers of intelligence and security services in the field of national security, the coordination of performance of these services, their processing of data, national and international cooperation in these services, and the exercise of supervision and treatment of complaints and confidentiality.[79] Certain portions of the new Act entered into force on September 1, 2017.[80]

Although the Act was passed "with broad support," the rights group Bits of Freedom reportedly cautioned that "the Netherlands' military and civil intelligence agencies will now have the opportunity to tap large quantities of internet data traffic, without needing to give clear reasons and with limited oversight," and expressed opposition to the Act's "three-year term for storage of data that agencies deem relevant, and the possibility for them to exchange information they cull with foreign counterparts."[81] Government officials contend, however, that the augmented powers "are needed to counter threats to national security in the modern era, and their use can be tested by an oversight panel."[82] A government press release, while noting that the Dutch

---

[75] *Id.*

[76] Van der Eijk, *supra* note 9; Article 29 Working Party, 693/14/EN WP 213, Opinion 03/2014 on Personal Data Breach Notification (adopted Mar. 25, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf, *archived at* https://perma.cc/PTN2-UYMQ.

[77] Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017) [Act of 26 July 2017, Containing Rules on the Intelligence and Security Services and Amendment of Some Other Laws (Intelligence and Security Services Act 2017)] (Wiv), STB. No. 317 (Aug. 17, 2017), https://www.eerstekamer.nl/9370000/1/j9vvkfvj6b325az/vkgudfl6pgy4/f=y.pdf, *archived at* https://perma.cc/C3WN-AG2F.

[78] *Dutch Pass 'Tapping' Law, Intelligence Agencies May Gather Data en Masse*, CETUSNEWS.COM (July 11, 2017), http://www.cetusnews.com/news/Dutch-pass-%27tapping%27-law--intelligence-agencies-may-gather-data-en-masse.rJeqq_0Mrb.html, *archived at* https://perma.cc/NL6T-3W97.

[79] Wiv, preamble.

[80] Besluit van 19 augustus 2017 tot vaststelling van het tijdstip van inwerkingtreding van enkele onderdelen van de Wet op de inlichtingen- en veiligheidsdiensten 2017 [Decision of 19 August 2017 Determining the Date of Entry into Force of Some Parts of the Intelligence and Security Services Act 2017], STB. No. 318 (Aug. 25, 2017), https://www.eerstekamer.nl/9370000/1/j9vvkfvj6b325az/vkh37qglhlye/f=y.pdf, *archived at* https://perma.cc/M2TR-XHXX.

[81] *Dutch Pass 'Tapping' Law, Intelligence Agencies May Gather Data en Masse*, *supra* note 78.

[82] *Id.*

intelligence and security services (AIVD and MIVD) would now have the power to investigate cable and other types of telecommunications, contended that there are strong safeguards to ensure that the use of the agencies' powers is always legitimate, including by conducting independent testing in advance.[83]

Articles 32–35 have to do with the establishment, terms of reference, task assignment, composition, and other special provisions with regard to a review committee, comprised of three members (including a chairman) that has the power to review permission given by the relevant Minister in regard to such activities as observing and recording data about natural persons or things, tracking and recording data about natural persons or things, and so on. The review committee's decisions are binding.[84] Article 97 now provides for a supervisory committee for the intelligence and security services that incorporates the already extant supervision department (to supervise the legality of execution of acts taken pursuant to the Act) and the complaints-handling department.[85] Articles 98–106 and 170 are on the functioning of the new supervisory committee.

On November 1, 2017, the Electoral Council (Kiesraad) of the Netherlands publicly announced that a referendum will be held within six months, based on the more than 384,000 signatures received, on the Act on Intelligence and Security Services.[86] The Council of State (Raad van Staat) has ruled that an appeal made against the Electoral Council decision admitting the final request to hold the consultative referendum is inadmissible; therefore the Electoral Council's Referendum Commission can proceed to set the date for the referendum.[87]

The Consultative Referendum Act sets a threshold of 300,000 signatures as necessary for holding a public vote.[88] Since the Consultative Referendum Act came into force in 2015, it has become

---

[83] Press Release, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Eerste Kamer stemt in met nieuwe Wet op de inlichtingen- en veiligheidsdiensten [First Chamber Votes in Favor of New Law on Information and Security] (July 11, 2017), https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijks relaties/nieuws/2017/07/11/eerste-kamer-stemt-in-met-nieuwe-wet-op-de-inlichtingen--en-veiligheidsdiensten/, *archived at* https://perma.cc/C56C-FQQQ.

[84] Wiv arts. 32 & 33.

[85] *Id*. art. 97 paras. 1 & 2.

[86] Press Release, Kiesraad, Referendum over Wiv gaat door [Referendum on Wiv Continues] (Nov. 1, 2017), https://www.kiesraad.nl/actueel/nieuws/2017/11/01/referendum-over-wiv-gaat-door, *archived at* https://perma.cc/R7J6-E6TU. According to the Electoral Council, it is likely that the referendum will coincide with the holding of municipal elections on March 21, 2018. *Id*. *See also* Kenneth Hall, *Netherlands to Hold Referendum on Surveillance Law*, JURIST PAPER CHASE (Nov. 1, 2017), http://www.jurist.org/paperchase/2017/11/netherlands-to-hold-referendum-on-surveillance-law.php, *archived at* https://perma.cc/LUG3-5GHL.

[87] Press Release, Kiesraad, Beroep niet-ontvankelijk: referendum Wiv definitief [Action Inadmissible: Wiv Referendum Final] (Nov. 10, 2017), https://www.kiesraad.nl/actueel/nieuws/2017/11/10/beroep-tegen-besluit-over-referendum-wiv-niet-ontvankelijk, *archived at* https://perma.cc/N3HC-V5KP.

[88] Wet van 30 september 2014, houdende regels inzake het raadgevend referendum (Wet raadgevend referendum) [Act of 30 September 2014, Concerning Rules for the Consultative Referendum (Consultative Referendum Act] (*as last amended* effective Apr. 1, 2017), art. 2, http://wetten.overheid.nl/BWBR0036443/2017-04-01, *archived at* https://perma.cc/X4A4-ZJ4K.

possible for almost all parliamentary laws and approved treaties to be put to a referendum.[89] According to the Electoral Council, this is the second time that both the introductory phase (with at least 10,000 valid requests) and the final phase (with at least 300,000 valid requests) for holding a referendum has been reached. The first time was the referendum on a partnership agreement with Ukraine.[90] The outcome of a referendum is only an advisory verdict for rejection of a law if the majority votes in favor of rejection with at least 30% of the total number of eligible voters taking part.[91]

E. Data Retention Act Voided

The Guardian reported in March 2015 that a judge in The Hague had struck down the 2009 Data Retention Act, stating that the Dutch regime for retention of telephone and internet user data helps in solving crime "but is too intrusive" and breaches the privacy of telephone and internet users.[92] The ruling followed a similar decision issued in April 2014 by the Court of Justice of the European Union that did away with EU data collection legislation it found to be too broad and lacking in sufficient privacy safeguards.[93]

III. Other Developments

On November 21, 2017, the Dutch Senate adopted an act to the effect that the registration data of vehicles that have recently passed by an Automatic Number Plate Recognition (ANPR) camera at certain locations on public roads "may be stored for four weeks."[94] According to the Ministry of Justice and Security,

> ANPR … is important for the purposes of investigating serious offences for which it does not emerge until further down the line that information about a vehicle plays a role. Such information could be crucial in cases of using explosives to target ATMs, abductions, human trafficking and terrorism. ANPR can also help in efforts to apprehend fugitives.[95]

---

[89] Press Release, Kiesraad, Referendum over Wiv gaat door, *supra* note 86.

[90] *Id.*

[91] Wet raadgevend referendum art. 3.

[92] *Data Retention: Netherlands Court Strikes Down Law As Breach of Privacy*, THE GUARDIAN (Mar. 11, 2015), https://www.theguardian.com/technology/2015/mar/12/data-retention-netherlands-court-strikes-down-law-as-breach-of-privacy, *archived at* https://perma.cc/ZK2R-RQB5.

[93] *Id.*; David Meyer, *Dutch Court Suspends Metadata Surveillance Law over Privacy*, TECHEU, http://tech.eu/news/dutch-court-suspends-data-retention-law/ (last visited Dec. 14, 2017), *archived at* https://perma.cc/ML8E-EHPD; Danny O'Brien, *Data Retention Directive Invalid, Says EU's Highest Court*, ELECTRONIC FRONTIER FOUNDATION (Apr. 8, 2014), https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court, *archived at* https://perma.cc/27FA-PMHS.

[94] Press Release, Ministry of Justice and Security, Senate Supports Storing Vehicle Registration Data (Nov. 21, 2017), https://www.government.nl/ministries/ministry-of-justice-and-security/news/2017/11/21/senate-supports-storing-vehicle-registration-data, *archived at* https://perma.cc/ZX5X-XU7N.

[95] *Id.*

Because vehicle registration data might provide important clues for identifying suspects and tracking down their home addresses,

> the police are being given the option of investigating what vehicles were driving at the scene of a crime as well as where the suspect's vehicle came from or headed to. This ability to look back at recorded data is new. The police are not currently authorised to store the number plate data of all vehicles passing a camera and consult that data retrospectively.[96]

The Ministry states that the legislation has safeguards to ensure road users' data protection; for example, the number plate data may only be gathered "on public roads and in locations relevant to investigatory activities," namely "airports as well as ports, car parks alongside motorways and border crossings," and there will be careful control of access to the vehicle registration data.[97] In addition, the access will be given only to "specially authorised investigative officers … at the behest of the public prosecutor," with the information consultable only in order to investigate serious crimes and apprehend fugitives.[98] The authorities will also annually publish a camera site plan specifying the permanent cameras' exact location.[99]

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

Portugal

Eduardo Soares
Senior Foreign Law Specialist

In 1995 the European Union issued Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive).[1] To transpose Directive No. 95/46/EC into its domestic legislation, Portugal enacted Law No. 67 of October 26, 1998, which became its law on the protection of personal data.[2]

On April 26, 2016, the European Union issued Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.[3] According to article 94 of Regulation 2016/679, Directive 95/46/EC will be effectively revoked on May 25, 2018. Portugal has yet to enact legislation that revokes Law No. 67/98 and transposes Regulation (EU) 2016/679 into its domestic legal system.

On April 27, 2016, the European Union issued Directive 2016/680[4] on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data. The Directive entered into force on May 5, 2016.[5] According to article 63, EU Member States have until May 6, 2018, to transpose this Directive into their domestic legal systems.[6] Portugal has yet to enact legislation to this effect.

---

[1] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at* https://perma.cc/P5FP-2RR8.

[2] Lei No. 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais [Personal Data Protection Law], http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=156&tabela=leis&ficha=1&pagina=1, *archived at* https://perma.cc/SQF7-YXAS.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1509458857466&from=EN, *archived at* https://perma.cc/4HPB-DXKW.

[4] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Criminal Law Enforcement Data Protection Directive), 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN, *archived at* https://perma.cc/7SZF-EQKX.

[5] *Id*. art. 64.

[6] *Id*. art. 63.

Spain

Graciela Rodriguez-Ferrand
Senior Foreign Law Specialist

SUMMARY The most significant development regarding online privacy in Spain since 2012 has been the decision rendered by the European Court of Justice in *Google Spain*, which basically ruled that Google had an obligation to remove links to pages displayed by third parties. Regarding data retention, the prior law was amended to require that the transfer of data to qualified authorities may only be done through electronic means and limited to the information that is essential for the detection, investigation, and prosecution of serious crimes. The Penal Code was also amended to include new cybercrimes and amend some of the provisions already in force related to online privacy, such as computer intrusion and sexting.

The most significant development related to the right of privacy in Spain since 2012 has been the European Court of Justice (ECJ) decision rendered in the *Google Spain* case on May 13, 2014.[1] In that case the ECJ determined that search engines are engaged in the processing of data because they navigate the internet in an automatic, continuous, and systematic manner searching for information.[2] The decision further established that since Google, a US-based company, had a Spanish subsidiary, it was subject to EU law because it operated as an establishment in Spain and carried out its commercial transactions there through advertising space accessible in its search engine.[3]

Based on EU legislation and specifically EU Directive 95/46 on Data Protection,[4] the ECJ ruled that Google had an obligation to remove links to pages displayed by third parties, in this case *La Vanguardia* newspaper, when they became inadequate, irrelevant, or excessive in relation to the purposes for which they were collected by the mere fact of the passage of time, even if the content published by the third parties was lawful.[5]

The ECJ also recognized the right of individuals to request that search engines remove links to personal data. It concluded that there was not a preponderant public interest in access to the links offered by the search engine related to auction notices for a debt that was settled sixteen

---

[1] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T.

[2] JUAN PABLO APARICIO VAQUERO & ALFREDO BATUECAS CALETRIO, EN TORNO A LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS EN LA SOCIEDAD DE LA INFORMACIÓN 81 (Granada, 2015).

[3] *Id*.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046, *archived at* https://perma.cc/MB6S-347M.

[5] APARICIO VAQUERO & BATUECAS CALETRIO, *supra* note 2, at 82.

years before that outweighed the plaintiff's privacy interests. Therefore, the court granted the plaintiff the right to demand that the search engine erase all search-result links to his name and the 1998 auction legal notices.[6] However, the decision also established that the right to be forgotten is not without limitations.[7] Determining the proper balance between the privacy rights of an individual affected and the legitimate interest of a search engine may depend on the type of information involved, such as the sensitivity of the information for the privacy of the individual in question, the public interest in access to the information, and the status of the individual in the public sphere, the ECJ said.[8]

Since the *Google v. Spain* decision, anyone in Spain who wants to have search results related to personal data removed must make a direct claim to the search engine in question, which must then decide on a case-by-case basis whether there are justified grounds for the request.[9] Requests are deemed justified if the individual's right of privacy takes precedence over the public's interest in accessing such information.[10] If the petition is denied, the petitioner may seek redress through the courts.[11] As a consequence of the decision, search engines such as Google, Yahoo, and others now offer users a special form to request the removal of links according to data protection standards.[12]

Regarding data retention, Law 25/2007[13] was amended by Law 9/2014,[14] which now requires that the transfer of data to qualified authorities be done only through electronic means and be limited to the information that is essential for the detection, investigation, and prosecution of serious crimes.[15]

In addition, the Penal Code was amended by Law 1/2015[16] to include new cybercrimes and amend some of the provisions already in force related to online privacy. Computer intrusion, or accessing or facilitating access to an information system by circumventing security measures and without proper authorization, is now punishable with a term of imprisonment ranging from three

---

[6] *Id*. at 83.

[7] *Id.*

[8] *Id*. at 85–86.

[9] *Id*. at 90.

[10] *Id.*

[11] *Id.*

[12] *Id*.

[13] Ley 25/2007 de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, BOLETÍN OFICIAL DEL ESTADO [B.O.E.], Oct. 19, 2007, http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243&b=9&tn=1&p=20140510, *archived at* https://perma.cc/4NAK-MH8P.

[14] Ley 9/2014 de Telecomunicaciones, B.O.E., May 10, 2014, http://www.boe.es/boe/dias/2014/05/10/pdfs/BOE-A-2014-4950.pdf, *archived at* https://perma.cc/733Q-6D48.

[15] *Id.* art. 22.2.

[16] Ley Orgánica 1/2015 por la que se Modifica la Ley Orgánica 10/1995, de 23 de Noviembre, del Código Penal, B.O.E., Mar. 31, 2015, https://www.boe.es/buscar/act.php?id=BOE-A-2015-3439, *archived at* https://perma.cc/TA2T-BW79.

months to two years and a fine.[17] The same punishment applies to the interception of non-public transmissions of computer data, which is a new crime.[18] Those who manufacture, acquire, import, or provide others, without authorization, the tools or instruments to carry out the crimes of computer intrusion and computer data interception, such as a computer program adapted to perpetrate a crime or a computer password or access key allowing access to a computer system, are subject to imprisonment for six months to two years and a fine.[19]

The abovementioned crimes now carry an enhanced penalty of a fine ranging from €5,400 to €1,800,000 (about US$6,350 to $2,117,000) when they are perpetrated by a criminal organization[20] or when criminal responsibility falls on a company or legal entity.[21]

The collection of personal data in violation of someone's privacy now carries an enhanced penalty of imprisonment of three to five years when it is carried out by those in charge of or responsible for electronic files, archives, or registries,[22] and through the unauthorized use of personal information of the victim.[23] If the personal information is disseminated, transferred, or revealed to third persons, the perpetrator will be subject to the upper half of the sanction.[24] If the personal information involved in the crime reveals the ideology, religion, beliefs, health, racial origin, or sexuality of the victim, or if the victim is a minor or disabled person, the perpetrator will be subject to the upper half of the sanction.[25] The same increased sanction will apply if the crime is perpetrated for profit.[26]

"Sexting" is now a crime punishable with imprisonment for three months to one year and a fine.[27] It is defined as the unauthorized transfer or exposure to third persons of images or audiovisual recordings of the victim, even when they were taken with his or her consent in a residence or a private setting.[28] Sexting will be considered an aggravated crime if it is carried out by a spouse or a person that is or was in an affectionate relationship in the past with the victim even if they did not live together, if the victim is a minor or disabled, or if the crime was

[17] *Id*. art. 197 *bis*, para. 1.

[18] *Id.* art. 197 *bis*, para 2.

[19] *Id*. art. 197 *Ter*.

[20] *Id*. art. 197 *Quarter*.

[21] *Id.* arts. 50.4 & 197 *Quinquies*.

[22] *Id.* art. 197. 4.a.

[23] *Id*. art. 197.4.b.

[24] *Id.* art. 197.4.b, para. 2.

[25] *Id.* art. 197.5.

[26] *Id*. art. 197.6.

[27] *Id.* art. 197.7, para. 1.

[28] *Id.*

carried out for profit.[29] In such cases, the perpetrator will be subject to the upper half of the sanction.[30]

The Agencia Espanola de Protección de Datos (AEPD) (Spanish Agency for Data Protection) has recently imposed economic sanctions of €1.2 million (about US$1.4 million) on Facebook for violations of the Ley Organica de Protección de Datos de Carácter Personal.[31] According to the decision, the data protection agency of Spain concluded that Facebook collects the personal data of Facebook users without the informed, specific, and unequivocal consent of those users, as required by Spanish law, for economic gain.[32] The agency further concluded that Facebook shares the users' personal information with advertisers and marketers without informing users. During the investigation, the AEPD found that the social networking company collects sensitive data referring to users' ideology, sex, religious beliefs, personal preferences, and navigation habits without clearly informing them about how that information will be used and for what purpose.[33]

The AEPD has published on its website an updated guide on the data protection rights of citizens, which compiles all the rights and procedures for their enforcement, in furtherance of the policies established in the *AEPD Strategic Plan 2015–2019 on Data Protection*.[34]

---

[29] *Id.* art. 197.7, para. 2.

[30] *Id.*

[31] AEPD, Resolución R/01870/2017 en Procedimiento Sancionador PS/00082/2017 (Sept. 2017), http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2017/common/pdfs/PS-00082-2017_Resolucion-de-fecha-21-08-2017_Art-ii-culo-4-5-6-7-LOPD.pdf, *archived at* https://perma.cc/KVT4-QHMC; Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal [Law on Personal Data Protection], B.O.E., Dec. 14, 1999, http://www.agpd.es/portalwebAGPD/canaldocumentacion/ legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos__Consolidado.pdf, *archived at* https://perma.cc/N3MM-XMLE.

[32] Press Release, AEPD, La AEPD Sanciona a Facebook por Vulnerar la Normativa de Protección de Datos (Sept. 11, 2017), https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-iden-idphp.php, *archived at* https://perma.cc/G6UW-4PRQ.

[33] *Id.*

[34] *Guia del Ciudadano*, AEPD, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf, *archived at* https://perma.cc/H6Z6-X7R5; *Plan Estratégico 2015-2019*, AEPD, http://www.agpd.es/portalwebAGPD/LaAgencia/common/Resolucion_Plan_Estrategico.pdf, *archived at* https://perma.cc/EE7H-Q8SQ.

Sweden

Elin Hofverberg
Foreign Law Research Consultant

SUMMARY Since 2012 Sweden has made a number of changes to its privacy regulation and interpretations. Most of these changes have been in response to European Union measures, such as the 2014 decision by the European Court of Justice (ECJ) invalidating the Data Retention Directive, the "right to be forgotten" case from 2014, and upcoming legislation in relation to the EU's General Data Protection Regulation, which will apply directly in all EU countries starting on May 25, 2018. There have also been a number of precedent cases in which the Swedish Supreme Court has determined how personal data should be protected online. In 2016, the ECJ found that the Swedish data retention rules violate EU law.

I. Introduction

There have been a number of developments in privacy law in Sweden since 2012. The biggest change is yet to come, however, as the European Union's General Data Protection Regulation (GDPR) will apply directly in Sweden and the remaining EU Member States beginning on May 25, 2018.[1] For instance, the Personal Data Act (Personuppgiftslagen, PUL)—the centerpiece of Swedish privacy legislation—will be replaced by this EU regulation, which has caused a number of add-on amendments to be introduced. This report focuses on changes in force as of December 2017 and only briefly mentions the likely effects of the GDPR on Swedish legislation. Ongoing work to comply with GDPR and the EU Law Enforcement Directive[2] can be found on the Swedish government and Swedish Parliament websites.[3]

---

[1] See EU survey for details.

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (EU Law Enforcement Directive), 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG, *archived at* https://perma.cc/SEK4-VSKN.

[3] Statens Offentliga Urtredningar [SOU] 2017:39 Ny dataskyddslag - Kompletterande bestämmelser till EU:s dataskyddsförordning, http://www.regeringen.se/49a184/contentassets/e98119b4c08d4d60a0a2d0878990d5ec/ny-dataskyddslag-sou-201739, *archived at* https://perma.cc/7D9P-6CS4. For example, Datainspektionen (the Swedish Data Protection Authority) has critiqued the government committees for not recognizing the difference between a directive and a regulation, noting that Swedish legislators are trying to keep much of Sweden's personal data legislation in place by arguing that the laws in force correspond to the GDPR. Datainspektionen, Remissvar, Remittering av betänkandet SOU 2017:66 Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning 1–2 (Nov. 1, 2017), http://www.datainspektionen.se/Documents/remissvar/2017-11-13-yttrande-socialdataskyddsutredningen.pdf, *archived at* https://perma.cc/MZ8K-VXTD; Datainspektionen, Datainspektionen pekar på vikten att lagförslag ger tillräckligt rättsligt stöd (Nov. 13, 2017), https://www.datainspektionen.se/press/nyheter/2017/datainspektionen-pekar-pa-vikten-att-lagforslag-ger-tillrackligt-rattsligt-stod/, *archived at* https://perma.cc/FJ9N-QLBQ.

II. Legislative Changes

A. Implementation of the Data Retention Directive

As mentioned in the Law Library of Congress's 2012 report,[4] the Swedish Parliament passed a bill to implement the EU Data Retention Directive, including its crime-fighting provisions, in May 2012.[5]

B. Adoption of Secret Surveillance Measures

In 2014 the Swedish Parliament adopted rules that allowed for an increase in secret surveillance measures, making temporary tools permanent.[6] For example, the new rules include allowing secret surveillance of electronic communications involving spousal relationships when investigating terrorism-related crimes or crimes that carry a minimum two-year prison sentence.[7]

Finding a balance between security and personal integrity continues to be subject to debate within the Swedish Parliament. Members of Parliament are currently discussing new privacy protections during signal surveillance for defense purposes.[8]

C. Personal Data Act

There have been no amendments to Sweden's principal Personal Data Act, the PUL, since 2010.[9] However, the law is set to be repealed in May 2018 when the GDPR will apply directly.[10] One of the more notable changes that will take place is that the frequently used section 5a PUL exception (commonly referred to as *missbruksregeln*, or the "abuse rule"[11]) will no longer be

---

[4] ELIN HOFVERBERG & EDITH PALMER, ONLINE PRIVACY LAW: SWEDEN (Law Library of Congress, June 2012), https://www.loc.gov/law/help/online-privacy-law/sweden.php.

[5] LAG OM INHÄMTNING AV UPPGIFTER OM ELEKTRONISK KOMMUNIKATION I DE BROTTSBEKÄMPANDE MYNDIGHETERNAS UNDERRÄTTELSEVERKSAMHET [ACT ON COLLECTION OF DATA INFORMATION ON ELECTRONIC COMMUNICATIONS FOR THE CRIME PREVENTION AUTHORITY'S SURVEILLANCE ACTIVITY] (SFS 2012:278), http://www.notisum.se/rnp/sls/lag/20120278.htm, *archived at* https://perma.cc/QA57-ZU5Q.

[6] Proposition [Prop.] 2013/14:237 Hemliga tvångsmedel, http://www.regeringen.se/49bb7b/contentassets/cc6ff48d963b40cea1eebed07ba09644/hemliga-tvangsmedel-mot-allvarliga-brott-prop.-201314237, *archived at* https://perma.cc/9AB9-8LJ4.

[7] 27 kap. 2§ 2st 1-8 RÄTTEGÅNGSBALKEN [RB], http://www.notisum.se/rnp/sls/lag/19420740.htm, *archived at* https://perma.cc/7YNA-N9UT.

[8] Skrivelse[Skr.] 2016/17:70 Signal spaning Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, http://www.riksdagen.se/sv/dokument-lagar/dokument/skrivelse/integritetsskydd-vid-signalspaning-i_H40370, *archived at* https://perma.cc/5KVW-TE6S; Försvarsutskottets betänkande[Bet.] 2016/17:FöU5 - Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, http://www.riksdagen.se/sv/dokument-lagar/arende/betankande/integritetsskydd-vid-signalspaning-i_H401FöU5, *archived at* https://perma.cc/PWF2-BT5Q.

[9] PERSONUPPGIFTSLAG [PUL] [PERSONAL DATA ACT] (SFS 1998:204), http://www.notisum.se/rnp/sls/fakta/a9980204.htm, *archived at* https://perma.cc/87ZA-Z7V2.

[10] *See* EU survey.

[11] 5a§ PUL.

valid, as the GDPR does not allow for such an exception.[12] This exception currently allows for the use of personal data in texts, such as references on a blog or in an email, without triggering the procedural requirements in the PUL, as long as the use does not violate the integrity of the subject.[13]

D. New Rules on Sharing Personal Information Within the EU

Sweden implemented Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[14] in May of 2013, effective June 1, 2013.[15] This will be replaced by implementation of the EU Law Enforcement Directive in May of 2018.

E. Changes in Electronic Communications

Since 2012 there have been ten amendments to the Swedish Electronic Communications Act (Lag om elektronisk kommunikation, LEK)—the law that contains the data retention provisions.[16] None of them pertain to privacy protections for online data or data retention, however.

III. ECJ Limits Swedish Data Retention Provisions

The Swedish data retention provisions found in the LEK legislation implement EU Directive Nos. 2006/24/EC and 2002/58/EC, of which the 2006/24/EC Directive was struck down by the European Court of Justice (ECJ) in 2014 in the *Digital Rights Ireland* case.[17] The Swedish authorities, over the objection of several internet service providers (ISPs), continued to mandate retention of user data for six months, with reference to the domestic LEK legislation (as based on

---

[12] *Missbruksregeln upphör*, DATAINSPEKTIONEN, Feb. 23, 2017, https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/, archived at https://perma.cc/4BDS-UTDL.

[13] *Id.*

[14] Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008 O.J. (L 350) 60, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977, *archived at* https://perma.cc/5NWY-KWX8.

[15] LAG MED VISSA BESTÄMMELSER OM SKYDD FÖR PERSONUPPGIFTER VID POLISSAMARBETE OCH STRAFFRÄTTSLIGT SAMARBETE INOM EUROPEISKA UNIONEN (SFS 2013:329), http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2013329-med-vissa-bestammelser-om-skydd_sfs-2013-329, *archived at* https://perma.cc/QM2K-LV5K.

[16] *See* list of amendments available, *Lag (2003:389) om elektronisk kommunikation*, NOTISUM, http://www.notisum.se/rnp/sls/fakta/a0030389.htm, *archived at* https://perma.cc/7GCQ-42GH; LAG OM ELEKTRONISK KOMMUNIKATION [LEK][ACT ON ELECTRONIC COMMUNICATIONS](SFS 2003:389), NOTISUM, http://www.notisum.se/rnp/sls/lag/20030389.htm, *archived at* https://perma.cc/7HSR-86V9.

[17] Joined Cases C-293/12 and C-594/12, Dig. Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/XZK2-Y7D5; *see also* EU survey.

EU Directive 2002/58/EC).[18] ISP Tele2 refused to follow these rules, citing the ECJ ruling,[19] resulting in litigation in the Swedish courts.[20]

In December of 2016, a preliminary ruling was delivered by the ECJ in which it determined that the Swedish rules for data retention were too general and indiscriminate, as it called for the retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communications.[21] In March 2017, the Administrative Court of Appeals that had referred the question to the ECJ concluded that Swedish ISPs need not retain data on their customers for investigative reasons.[22] The Swedish Justice Department has prepared a committee report with the purpose of determining how the data retention provisions can be amended to harmonize and comply with the EU legislation.[23] The government report (the next step in the legislative process) is currently on referral (*remissyttrande*) with stakeholders.[24] Responses must be received by January 30, 2018.[25] Work is also being done at the EU level to replace provisions of Directive 2006/24/EC.[26]

---

[18] Kammarrätten i Stockholm [Administrative Appeals Court Stockholm], 7380-14 p. 2, http://www.kammarrattenistockholm.domstol.se/Domstolar/kammarrattenistockholm/Domar/2017%20jan-juni/Dom_7380-14.pdf, *archived at* https://perma.cc/3Q48-6NQD.

[19] *Id*.

[20] *Id*.

[21] Joined Cases C-203/15, Tele2 Sverige AB v. Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v. Tom Watson, paras. 75–81, ECLI:EU:C:2016:970, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 62015CJ0203, *archived at* http://perma.cc/PT73-PD2J, *summarized in* Elin Hofverberg, *European Court of Justice/Sweden: Invalidation of Data Retention Obligations*, GLOBAL LEGAL MONITOR (Jan. 19, 2017), https://www.loc.gov/law/foreign-news/article/european-court-of-justicesweden-invalidation-of-data-retention-obligations/, *archived at* https://perma.cc/6P7S-HRCP.

[22] Kammarrätten i Stockholm [Administrative Appeals Court Stockholm], 7380-14, http://www.kammarrattenistockholm.domstol.se/Domstolar/kammarrattenistockholm/Domar/2017%20jan-juni/Dom_7380-14.pdf, *archived at* https://perma.cc/EEZ2-4UKU; Press Release, Kammarrätten i Stockholm, Post- och telestyrelsen (PTS) har inte haft rätt att förelägga Tele2 att lagra trafikuppgifter m.m. för brottsbekämpande ändamål, s.k. datalagring (Mar. 7, 2017), http://www.kammarrattenistockholm.domstol.se/Om-kammarratten-/Nyheter-och-pressmeddelanden/Post--och-telestyrelsen-PTS-har-inte-haft-ratt-att-forelagga-Tele2-att-lagra-trafikuppgifter-mm-for-brottsbekampande-andamal-sk-datalagring, *archived at* https://perma.cc/6NDT-TPYU.

[23] Dir. 2017:16 Datalagring och EU-rätten, http://www.regeringen.se/491d4e/contentassets/423c9145c0354e7aa7a8bf4657631dfe/datalagring-och-eu-ratten-dir.-201716, *archived at* https://perma.cc/CDW8-HT93; SOU 2017:75 Datalagring – brottsbekämpning och integritet, http://www.regeringen.se/4a8d12/contentassets/b635202b96fc4e4490886e0ef8601e66/datalagring--brottsbekampning-och-integritet-sou-201775, *archived at* https://perma.cc/EZ6V-VDAW.

[24] Remiss Ju2017/07896/Å, Regeringskansliet (Oct. 30, 2017), http://www.regeringen.se/4ab456/contentassets/a3e8bb4742c64e99baf0bc71c65dae9d/remisslista-sou-201775-datalagring--brottsbekampning-och-integritet, *archived at* https://perma.cc/X2WB-5SGY.

[25] *Id*. at 4.

[26] Communication from the Commission to the European Parliament, the European Council and the Council, *Fourth Progress Report Towards an Effective and Genuine Security Union*, COM (2017) 41 final (Jan. 25, 2017), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0041&from=EN, *archived at* https://perma.cc/Q7SK-93DS.

IV. Domestic Case Law

In 2015 the Administrative Supreme Court ruled on the limits of the section 5a missbruksregel in the PUL, determining that a list of personal information was covered by the rule, thus not making it a violation of how personal information may be handled.[27] The court found that the fact that the list was used when doing background checks on people was not material to whether the exception applied.[28]

In *NJA 2013 s. 1046* the Swedish Supreme Court found that publishing a copy of a judgment in a civil case online when the judgment contained the losing party's name and address violated the private data protections found in PUL.[29]

V. Guidance

Datainspektionen (the Swedish enforcement authority for PUL violations) has published GDPR guidance for personnel who work with personal data.[30]

VI. Information Held by the Government

A. Transfer of Private Information

In 2017 a government scandal pertaining to sensitive personal data was unveiled. Both the Transportation Authority (Transportstyrelsen) and the National Police (Rikspolisen) had transferred personal information from Sweden to be handled by private companies based in foreign countries.[31] A wave of criticism followed.[32] This incident also resulted in several members of Parliament reporting both the current and former governments to the

---

[27] Högsta förvaltningsdomstolen [HFD] [Administrative Supreme Court Reporter] 2015 ref. 3, http://www.hogstaforvaltningsdomstolen.se/Domstolar/regeringsratten/R%C%A4ttsfall/HFD%202015%20ref.%203.pdf, *archived at* https://perma.cc/Y933-EVGT.

[28] *Id*.

[29] NYTT JURIDISKT ARKIV [NJA][Supreme Court Reporter] 2013 s. 1046.

[30] Datainspektionen, Förberedelser inför EU:s dataskyddsförordning Vägledning till personuppgiftsansvariga, http://www.datainspektionen.se/Documents/vagledning-forberedelser-pua.pdf (last visited Dec. 11, 2017), *archived at* https://perma.cc/5SMB-2PZ8. Datainspektionen devotes an entire section of its website to the GDPR. *Dataskyddsförordningen*, DATAINSPEKTIONEN, http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/ (last updated Oct. 23, 2017), *archived at* https://perma.cc/LS94-U2BH.

[31] *Tidslinje: IT-skandalen på Transportstyrelsen*, SVERIGES RADIO (Aug. 28, 2017), http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6745040, *archived at* https://perma.cc/PRH4-MF8Y; Adrian Sadikovic, Daniel Öhman & Alexander Gagliano, *Rikspolischefen frångick säkerhetsskydds-förordningen*, SVERGIES RADIO (Sept. 5, 2017), http://sverigesradio.se/sida/artikel.aspx?artikel=6770725, *archived at* https://perma.cc/8P4E-G4WR.

[32] *E.g.*, Ulrica Olsson, *"Läckta personuppgifter kan handla om liv eller död,"* SVT (July 19, 2017), https://www.svt.se/nyheter/inrikes/lackta-personuppgifter-kan-handla-om-liv-eller-dod, *archived at* https://perma.cc/PF9Y-JACM.

Konstitutionsutskottet, the Constitutional Committee that scrutinizes the work of the government and decides whether a minister should be prosecuted, for how they handled the matter.[33]

B. Government Sale of Personal Information

In 2013 there was public criticism of Swedish government agencies for selling personal information.[34] Examples of government agencies that sold information included the tax authority, CSN (student loan agency), and Transportation Authority, with the latter making some SEK 30 million (approximately US$3.6 million) annually off of these sales.[35]

VII. Right to Be Forgotten

Swedes, based on Sweden being an EU Member State, are protected by the "right to be forgotten" as established in the ECJ *Google Spain* case from 2014.[36] This means that Swedes may ask Google and other search engines to remove content concerning them under certain circumstances.[37] According to reports, more than 11,000 claims had been lodged with Google by Swedish citizens as of May 2016.[38] For example, Google has so far removed content for a woman who wished to have her name and address removed.[39] Others have not found the same success. For example, a CEO who was linked to Hells Angels in an online article unsuccessfully brought suit the Svea Appeals Court to have that information removed from Google's top search results on him, as the court determined that the public interest outweighed the man's desire for the information to be forgotten.[40]

Swedish Datainspektionen has made a finding that Google may also have to remove content from its search results on searches made outside of the EU when the resulting information has

---

[33] For a list, see search results at RIKSDAGEN, https://www.riksdagen.se/sv/dokument-lagar/?doktyp=ku-anm&q=Transportstyrelsen&p=1&st=2 (last visited Nov. 29, 2017), *archived at* https://perma.cc/6KEZ-LYSF.

[34] *Kritik mot att myndigheter säljer personuppgifter*, SVERIGES RADIO (Aug. 4, 2013), http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5608445, *archived at* https://perma.cc/HF9R-4MC8; *Myndigheters försäljning av personuppgifter, Skriftlig fråga 2015/16:277*, RIKSDAGEN, https://www.riksdagen.se/sv/dokument-lagar/dokument/skriftlig-fraga/myndigheters-forsaljning-av-personuppgifter_H311277 (last visited Dec. 11, 2017), *archived at* https://perma.cc/K7ER-4UL2.

[35] *Kritik mot att myndigheter säljer personuppgifter*, SVERIGES RADIO, *supra* note 33.

[36] *See* EU survey.

[37] *Id*.

[38] Erik Wisterberg, *Så många svenskar kämpar för att bli bortglömda av Google* [*These Many Swedes Fight to Be Forgotten by Google*], BREAKIT (May 11, 2016), https://www.breakit.se/artikel/3667/sa-manga-svenskar-kampar-for-att-bli-bortglomda-av-google, *archived at* https://perma.cc/TA8R-5KCM.

[39] *Transparency Report*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview?privacy_requests=country:SE&lu=privacy_requests (last visited Nov. 21, 2017), *archived at* https://perma.cc/X25C-HP4U.

[40] Hanna Lundquist, *Granskad företagare får inte bli bortglömd* [*Scrutinized Businessman Not Allowed to Be Forgotten*], JOURNALISTEN (May 8, 2017), https://www.journalisten.se/nyheter/granskad-foretagare-far-inte-bli-bortglomd, *archived at* https://perma.cc/X2LD-P7PS.

connections to Sweden either because it is presented in the Swedish language, is stored on a Swedish website, or concerns a Swedish person.[41]

VIII. Outlook: The Swedish Constitution and GDPR

It is unclear what effects the GDPR will have on rights under the Swedish Constitution. The Constitution protects the right to privacy,[42] the right to free speech,[43] freedom of information,[44] and public access.[45] Any provision in the current PUL legislation is secondary to the Constitution,—i.e., any inconsistencies/discrepancies between the two and the protections found in two components of the Swedish Constitution, namely Tryckfrihetsförordningen (TF) (the Freedom of the Press Act) and Yttrandefrihetsgrundlagen (YGL) (the Fundamental Law on Freedom of Expression), will supersede protections in the PUL.[46] The GDPR, which is to replace the PUL, on the other hand, supersedes national legislation, including incompatible constitutional provisions. However, the Swedish government has interpreted the national discretion found in articles 85 and 86 of the GDPR regarding freedom of expression and freedom of information as allowing for Swedish constitutional protections in the YGL and TF in their current form to trump the GDPR,[47] arguing that the GDPR allows for a "national regulation of the relationship between protections for personal data on the one hand, and free speech, freedom of information and the right of public access on the other."[48] Whether that interpretation is correct is for the ECJ to determine.

---

[41] Press Release, Datainspektionen, The Right to Be Forgotten May Apply All Over the World (May 4, 2017), https://www.datainspektionen.se/press/nyheter/the-right-to-be-forgotten-may-apply-all-over-the-world/, *archived at* https://perma.cc/NT8D-42Z3.

[42] 2 kap. 6§ REGERINGSFORMEN [RF] [INSTRUMENT OF GOVERNMENT] [CONSTITUTION] (SFS 1974:152), http://www.notisum.se/rnp/sls/lag/19740152.htm, *archived at* https://perma.cc/Z47Y-5DSS.

[43] 2 kap. 1§ 1p. RF; 1 kap. 1 § YTTRANDEFRIHETSGRUNDLAG [YGL] [CONSTITUTION] (SFS 1991:1469), http://www.notisum.se/rnp/sls/lag/19911469.HTM, *archived at* https://perma.cc/5N5V-PPR3; 1 kap. 1 § TRYCKFRIHETSFÖRORDNING [TF] [CONSTITUTION] (SFS 1949:105), http://www.notisum.se/rnp/sls/lag/19490105.htm, *archived at* https://perma.cc/LYL6-HPYB.

[44] 2 kap. 1 § 2p. RF.

[45] 2 kap. 1 § TF.

[46] 1 kap. 7§ PUL.

[47] Kommittédirektiv [Dir. 2016:15] Dataskyddsförordningen, at 21f, https://www.regeringen.se/493ace/contentassets/b16563d102144523a1af80fb44321c43/dir.-201615-dataskyddsforordningen, *archived at* https://perma.cc/CGK8-FERJ.

[48] *Id*.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY Data protection legislation in the UK is primarily based upon directives from the European Union and aims to protect the rights of individuals to ensure that their personal information remains private and secure. Data retention is now governed by the Investigatory Powers Act 2016, which enables the Secretary of State to issue notices to telecommunications operators to retain certain communications data for up to twelve months under specified conditions. Regulations have been amended to give the Information Commissioner a broader range of sanctions to impose for regulatory breaches. A Data Protection Bill to follow but expand upon the European Union's General Data Protection Directive is pending.

I. Introduction

There have been a number of changes in the laws of the United Kingdom relating to data protection and online privacy since the Law Library of Congress published its report in 2012.[1] Many of these new legal provisions are about to be replaced by the pending Data Protection Bill, which will have a sweeping impact on how information is processed and stored.[2] This survey summarizes the changes that have occurred since 2012, the current law as it stands in December 2017, and anticipated changes under the pending Data Protection Bill.

II. Retention of Data

The retention of data has been an evolving area of the law. The Data Retention (EC Directive) Regulations 2009 was the subject of an adverse ruling that necessitated emergency legislation.[3] The Data Retention and Investigatory Powers Act 2014 and the regulations[4] made under it were expedited through Parliament and enacted as emergency legislation to fill the need created by the ruling; the legislation passed through Parliament in four days with cross-party support. It enabled the Secretary of State to issue a notice, with no judicial oversight, requiring telecommunications operators to retain a wide array of communications data for up to twelve

[1] CLARE FEIKERT-AHALT, ONLINE PRIVACY LAW: UNITED KINGDOM (Law Library of Congress, June 2012), https://www.loc.gov/law/help/online-privacy-law/uk.php, *archived at* https://perma.cc/TY3L-WHN5.

[2] Data Protection Bill, 2017-18, HL Bill 66, https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf, *archived at* https://perma.cc/P3GQ-9ZFF.

[3] Joined Cases C-293/12 and C-594/12, Dig. Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/XZK2-Y7D5.

[4] Data Retention and Investigatory Powers Act 2014, c. 27, § 1, https://www.legislation.gov.uk/ukpga/2014/27/enacted, *archived at* https://perma.cc/6QK3-FL8P; Data Retention Regulations 2014, SI 2014/2042, http://www.legislation.gov.uk/uksi/2014/2042/made, *archived at* https://perma.cc/2995-35ZA.

months.[5] The Act was subject to an adverse ruling from the European Court of Justice,[6] but also contained a sunset clause that caused it to expire at the end of 2016,[7] after which it was replaced by the Investigatory Powers Act 2016.[8]

A. Retention Notice to Telecommunications Operator

The Investigatory Powers Act enables the Secretary of State to issue a retention notice that requires a telecommunications operator to retain communications data for up to twelve months if two conditions can be met: the retention must be necessary and proportionate for one of ten specified purposes,[9] and a judicial commissioner must have approved the decision to issue the notice. Before issuing a notice, the Secretary of State must have considered the following:

> (a) the likely benefits of the notice,
> (b) the likely number of users (if known) of any telecommunications service to which the notice relates,
> (c) the technical feasibility of complying with the notice,
> (d) the likely cost of complying with the notice, and
> (e) any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates.[10]

---

[5] Data Retention and Investigatory Powers Act 2014, c. 27, § 1, https://www.legislation.gov.uk/ukpga/2014/27/enacted, *archived at* https://perma.cc/6QK3-FL8P.

[6] Joined Cases C-203/15, Tele2 Sverige AB v. Post-och telestyrelsen & C-698/15 Sec'y of State for the Home Dep't v. Watson, paras. 75–81, ECLI:EU:C:2016:970, http://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A62015CJ0203, *archived at* http://perma.cc/PT73-PD2J (holding that any data retention regime must comply with the principles of proportionality, necessity and legality). "Section 1 of DRIPA [Data Retention and Investigatory Powers Act] is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body." *Id.*

[7] *Id.* § 8.

[8] Investigatory Powers Act 2016, c. 25, https://www.legislation.gov.uk/ukpga/2016/25, *archived at* https://perma.cc/2MND-C769.

[9] Investigatory Powers Act 2016, c. 25, § 61(7)(a)–(j). It must be necessary to obtain the data,

> (a) in the interests of national security, (b) for the purpose of preventing or detecting crime or of preventing disorder, (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security, (d) in the interests of public safety, (e) for the purpose of protecting public health, (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, (h) to assist investigations into alleged miscarriages of justice, (i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition— (i) to assist in identifying P, or (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or (j) for the purpose of exercising functions relating to— (i) the regulation of financial services and markets, or (ii) financial stability. *Id.*

[10] Investigatory Powers Act 2016, c. 25, § 88, https://www.legislation.gov.uk/ukpga/2016/25, *archived at* https://perma.cc/2MND-C769.

The retention notice can apply to one, or a set description of, telecommunication operators.[11] Section 89 of the Act provides for the review of the Secretary of State's decision to issue a notice. The Judicial Commissioner must review the decision of the Secretary of State to ensure that it is necessary and proportionate applying the same principles that are used during an application for judicial review.

B. Type of Data to Be Retained

The type of data to be retained under the Investigatory Powers Act must be "relevant communications data," defined in the 2016 Act as data that can be used to identify, or used to assist in identifying, any of the following:

(a) the sender or recipient of a communication (whether or not a person),

(b) the time or duration of a communication,

(c) the type, method or pattern, or fact, of communication,

(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

(e) the location of any such system.[12]

Examples given of this type of data includes phone numbers, email addresses, and source IP addresses.[13] Internet connection records—that is, records such as websites visited or internet messaging application data—are specifically excluded from being retained under the provisions of the Investigatory Powers Act.

The exact type of data must be specified in the notice issued by the Secretary of State. It may include either a specified set of data, or all data from the operator for a specified period of time.[14]

C. Duration of Mandatory Retention of Data

Any notice must specify the period of time for which the data must be retained, which may not exceed twelve months. The length of time for which data may be retained varies according to the type of data. For specific communications the time period runs from the date on which the communication was sent. In other cases, the time period starts on the day the data is first held by the operator.[15]

---

[11] *Id*. § 88.

[12] *Id*. § 87(11).

[13] Investigatory Powers Act 2016, c. 25, Explanatory Notes, ¶ 265, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpgaen_20160025_en.pdf, *archived at* https://perma.cc/65FR-MAJR.

[14] Investigatory Powers Act 2016, c. 25, § 88.

[15] *Id*. § 87(3).

D. Cost of Retention

As noted above, before issuing a notice, the Secretary of State is required to consider the cost of compliance.[16] The 2016 Act requires the Secretary of State to put arrangements in place to ensure that telecommunications operators "receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate."[17] "Relevant costs" are those incurred when complying with the Investigatory Powers Act 2016. The amount the government may contribute varies according to the scope and extent of the arrangements; the Secretary of State may provide different levels of contributions according to the type of case.[18]

III. Sanctions for Regulatory Violations

The Information Commissioner (ICO) continues in his role of enforcing the data protection regulations. The Privacy and Electronic Communications (EC Directive) Regulations 2003 has been amended to lower the legal threshold at which the Information Commissioner can issue a civil monetary penalty for a serious breach of regulations 19 through 24. The threshold is now that any person is liable if he or she "knew or ought to have known that there was a risk that the contravention would occur,"[19] removing the requirement that the contravention must have been "of a kind likely to cause substantial damage or substantial distress,"[20] making it easier for the Information Commissioner to take action against individuals who seriously breach the marketing rules.[21]

The purpose of lowering the threshold was to enable the ICO to

> issue a wider range of smaller penalties, as well as being able to continue concentrating on larger cases. It is expected that this combined approach will have a more powerful effect on organisations that are breaking the law by making and sending unsolicited communications.[22]

---

[16] *Id*. § 88(1).

[17] *Id*. § 249(1).

[18] *Id*. § 249.

[19] Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015, ¶ 2(2), SI 2016/355, http://www.legislation.gov.uk/uksi/2015/355/made, *archived at* https://perma.cc/TD7Z-GST7.

[20] Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, Sched. ¶ 8A, http://www.legislation.gov.uk/uksi/2003/2426/made, *archived at* https://perma.cc/AW98-TDFB.

[21] Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015, SI 2016/355, http://www.legislation.gov.uk/uksi/2015/355/made, *archived at* https://perma.cc/TD7Z-GST7.

[22] Explanatory Memorandum to the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015, 2015 No. 355, ¶ 7.15, http://www.legislation.gov.uk/uksi/2015/355/pdfs/uksiem_20150355_en.pdf, *archived at* https://perma.cc/KN6W-TAQ6.

IV. Protection of Minors and Facebook

The government has continued to work to take steps to protect children when they engage in online activities. It recently commissioned a report by the UK Council for Child Internet Safety Evidence Group, which made a number of recommendations.[23] Of note in the report is the assessment that

> [a] range of industry initiatives exists in the form of agreements with the government, individual company policies and initiatives, and industry-level initiatives, but there is evidence to suggest that industry could do more to strengthen collaborative partnerships, particularly with law enforcement.[24]

V. Collection, Storage, and Use of Personal Data by Online Media or Services

The Privacy and Electronic Communications Regulations (EC Directive) (Amendment) Regulations 2016 amended the Privacy and Electronic Communications (EC Directive) Regulations 2003 to require anyone making a direct marketing telephone call to display their phone number without blocking caller ID.[25]

VI. European Union's Data Protection Directive

The European Union's General Data Protection Directive (GDPR) will apply in the UK beginning in May 2018.[26] In 2016, the UK government stated that it would implement the regulations in full[27] and on September 13, 2017, it introduced an almost two-hundred-page bill, known as the Data Protection Bill, which would repeal and replace the Data Protection Act 1998 and follow, but expand upon, the GDPR.[28] The intent behind the Data Protection Bill is to

---

[23] SONIA LIVINGSTONE ET AL., CHILDREN'S ONLINE ACTIVITIES, RISKS AND SAFETY, A LITERATURE REVIEW BY THE UKCCIS EVIDENCE GROUP (Oct. 2017), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf, *archived at* https://perma.cc/GV4N-PPDM.

[24] *Id*. at 4.

[25] Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2016, SI 2016/524, http://www.legislation.gov.uk/uksi/2016/524/made, *archived at* https://perma.cc/GN5C-8RX7.

[26] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) art. 4(1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

[27] 618 PARL. DEB., H.C. (5th ser.) (2016), *available at* https://hansard.parliament.uk/Commons/2016-12-12/debates/6EB0C615-2571-4B26-A75B-8CD1CF5FD854/EUDataProtectionRules, *archived at* https://perma.cc/VHU2-7ZM3.

[28] Data Protection Bill, 2017-18, HL Bill 66, https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf, *archived at* https://perma.cc/P3GQ-9ZFF.

"update data protection laws for the digital age."[29] Among other things, the Data Protection Bill will provide

- clarity on the definitions contained in the GDPR in the laws of the UK;
- stronger sanctions in cases of malpractice, enabling the Information Commissioner to impose administrative fines of up to £17 million (approximately US$22.5 million), or up to 4% of global turnover;
- the means for the Information Commissioner to bring criminal proceedings in cases where the data controller alters records to prevent disclosure to a subject access request;
- data processing for criminal justice agencies that will "[a]llow the unhindered flow of data internationally whilst providing safeguards to protect personal data";[30]
- new standards for the protection of general data, including providing individuals with rights to move or remove their personal data; and
- a new rule that establishes the age of thirteen as the minimum age at which parental consent is no longer needed to process data online.[31]

By addressing general data, processing of data by law enforcement, and data used to protection national security, the UK has stated that it is going beyond the requirements of the GDPR to set up a "bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes."[32]

---

[29] *Data Protection Bill 2017, Protection Bill 2017*. DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT (Sept. 14, 2017), https://www.gov.uk/government/collections/data-protection-bill-2017, *archived at* https://perma.cc/2QS2-RGU5.

[30] *Data Protection Bill Factsheet – Overview*, DEPARTMENT FOR DIGITAL, CULTURE MEDIA AND SPORT, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf (last visited Nov. 28, 2017), *archived at* https://perma.cc/7465-DGNH.

[31] *Id.*

[32] *Id.*