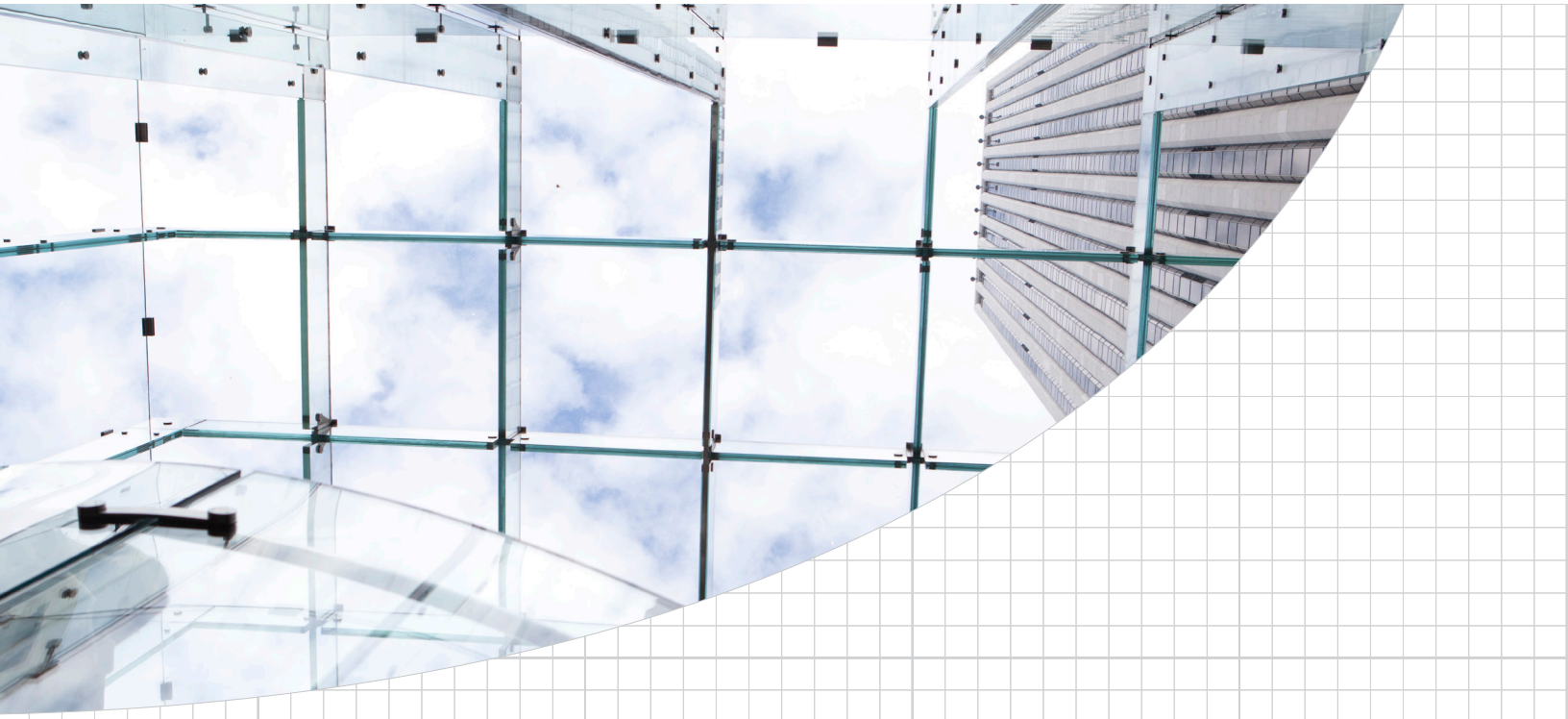
Bloomberg Law®

Privacy & Data Security Practice Portfolio Series
Portfolio No. 550
Section III: Information Notices and Data Subject Rights

EU General Data Protection Regulation

William RM Long
Geraldine Scali
Francesca Blythe

Sidley Austin LLP



Bloomberg BNA

PRIVACY & DATA SECURITY PRACTICE PORTFOLIO SERIES

EU GENERAL DATA PROTECTION REGULATION

by

William RM Long ● Geraldine Scali ● Francesca Blythe
Sidley Austin LLP
London

William RM Long, a Partner in the London office of Sidley Austin LLP, advises international clients on a wide variety of data protection, privacy, information security, social media, e-commerce, and other regulatory matters. Mr. Long is a member of the European advisory board of the International Association of Privacy Professionals (IAPP) and has experience with EU and international data protection and e-commerce projects working for clients in financial services and life sciences, as well as in other sectors.

Geraldine Scali is a Senior Associate in Sidley Austin's London office. Her main areas of practice are data protection, privacy, e-commerce, and information technology. She advises international clients on the implementation of global compliance data protection and privacy projects, social media, and on a broad range of data protection and privacy issues.

Francesca Blythe, an Associate in the London office of Sidley Austin LLP, advises international clients on a wide range of data protection and privacy issues and the implementation of data protection compliance projects. Her main areas of practice are data protection, privacy, e-commerce, and information technology.

The following cataloging data is provided by the Bloomberg BNA Library

Long, William RM.

EU General Data Protection Regulation.

(Privacy & data security practice series, ISSN 2333-0538; no. 550)
1. Data protection—Law and legislation—European Union countries. I. Scali, Geraldine. II. Blythe, Francesca. III. Title. IV. Series. V. Bloomberg BNA.
KF1263.C65 P74 no. 550
ISBN 978-1-63359-146-2

PORTFOLIO DESCRIPTION SHEET

EU General Data Protection Regulation

Privacy & Data Security Practice Portfolio Series No. 550, *EU General Data Protection Regulation*, provides in-depth insight into the legal considerations, compliance risks, and practical issues raised by the EU General Data Protection Regulation (the ''GDPR''). This portfolio is primarily designed to educate and guide in-house counsel and compliance, information security, and data protection officers of entities subject to the GDPR. The GDPR creates a single EU-wide law on data protection intended to increase legal certainty for individuals, businesses, and Data Protection Authorities (''DPAs'') and to contribute to the success of the EU's Digital Single Market. The GDPR also introduces the so-called ''one-stop-shop'' mechanism, which permits businesses that operate in more than one Member State to engage with a single Lead DPA and which is intended to promote harmonization and the Digital Single Market. Of particular significance is the extra-territorial application of the GDPR, where a non-EU based business will become subject to the GDPR when it is processing personal data of individuals in the EU as a result of offering goods or services to such individuals or monitoring their behavior. The GDPR also introduces significant new data protection requirements and rights for data subjects, as well as enforcement powers for DPAs, designed to ensure compliance, which include fines of up to 4% of annual worldwide turnover or €20 million, whichever is greater.

This portfolio may be cited as William RM Long, Geraldine Scali & Francesca Blythe, *EU General Data Protection Regulation*, 550 Privacy & Data Security Practice Portfolio Series (Bloomberg BNA).

PRIVACY & DATA SECURITY PRACTICE PORTFOLIO SERIES

This portfolio is part of Bloomberg BNA's Privacy & Data Security Practice Series, providing practice-oriented analytical content across a range of privacy and data security issues and practice areas. Each portfolio combines extensive research along with experienced practitioners' guidance and analysis. Areas of coverage include government enforcement, cloud computing, cross-border transactions, medical privacy, consumer financial privacy, and more. Portfolios in the series will be updated regularly.

Other Bloomberg BNA Products

Bloomberg BNA also has available the following publications:

Bloomberg Law: Privacy & Data Security brings you single-source access to the expertise of Bloomberg Law's privacy and data security editorial team, contributing practitioners, and in-country experts together with unmatched practice tools, including chart builders and detailed country profiles, to help you mitigate risk and quickly respond to client inquiries with confidence. *Bloomberg Law: Privacy and Data Security* provides you with practical guidance and tools to turn your strategy into action with connected primary sources, chart builders, customizable search tools, and global intelligence.

Privacy Law Watch™ provides comprehensive coverage every business day of the latest legal, regulatory, legislative, and judicial news in the privacy and security fields, including developments affecting data protection, employee privacy, data breaches, online and consumer privacy, identity theft, data retention, financial privacy, and health care privacy.

World Data Protection Report™ informs you of developments in the regulation of transactions involving privacy and information security around the world. It provides continually published news, commentary and expert analysis on privacy and data security laws worldwide, with a particular focus on issues such as cross-border data flows and drafting information security policies in compliance with international standards.

For further information on these or other Bloomberg BNA publications, call Customer Relations at: 1-800-372-1033, or visit our web site at: http://www.bna.com.

TABLE OF CONTENTS

III.

Information Notices and Data Subject Rights

Synopsis

Under the GDPR, data subjects must be provided with extensive information relating to the processing of personal data and are granted more extensive rights than under the Data Protection Directive. The data subject rights include:

(i) the right of subject access;
(ii) the right to erasure (''right to be forgotten'');
(iii) the right to restriction of processing;
(iv) the right to data portability;
(v) the right to object to processing; and
(vi) the right not to be subject to a decision based solely on automated processing (including profiling).

A. Information Notices

Article 13 of the GDPR sets out the information to be provided to a data subject at the time the personal data is obtained. These information requirements are much more extensive than under the Data Protection Directive and will require many controllers to review and amend their employee and customer notices, consents, and policies. According to Article 12 of the GDPR, this information should be provided in a ''concise, transparent, intelligible, and easily accessible form, using clear and plain language'' in particular when dealing with children. There is an exception to the provision of such information insofar as the data subject already has the information.[1]

The information to be provided free of charge pursuant to Article 13 of the GDPR includes:

(i) the identity and contact details of the controller and its DPO;
(ii) the purposes and legal basis for the processing and, if the processing is based on the legitimate interests ground, what the legitimate interests are;
(iii) the recipients of the personal data;
(iv) the details of any international transfers outside of the EEA;
(v) the retention period or, where this is not possible, the criteria used to determine this period;
(vi) the existence of the data subject's rights, including: the right of subject access, the right to rectification or erasure, the right to restriction of processing, the right to data portability, and the right to object to processing;
(vii) the existence of the right to withdraw consent to the extent this is the legal ground used for processing;
(viii) the right to lodge a complaint with the DPA;
(ix) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and
(x) the existence of automated decision-making, including profiling and ''meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.''[2]

Article 14 of the GDPR sets out the information to be provided where the personal data has not been obtained from the data subject. In addition to the information listed above as being required pursuant to Article 13, Article 14 requires that the source from which the personal data originated should also be provided.[3] This should be provided within one month of the receipt of the data, at the time of communication with the data subject, or when the data is first disclosed to a third party.[4] The information in Article 14 does not need to be provided where:

(i) the data subject already has the information;
(ii) the provision of the information proves impossible or would involve a disproportionate effort (for example, where the processing is for scientific and historical research purposes or statistical purposes), in which case the information should be made publicly available;
(iii) it is an EU or Member State legal requirement to obtain or disclose such data; or
(iv) the data must remain confidential pursuant to a statutory obligation of secrecy.[5]

Article 12(8) of the GDPR empowers the Commission to adopt delegated acts for the purpose of providing certain information in standardized icons, as well as the procedures for providing such icons. The concept of standardized icons was introduced in the proposal adopted by Parliament on March 12, 2014.[6] A standardized icon could show, for example, where personal data is encrypted or where personal data is not dis-

[1] Article 13(4) of the GDPR.

[2] Article 13 of the GDPR.

[3] Article 14(2)(f) of the GDPR.

[4] Article 14(3) of the GDPR.

[5] Article 14(5) of the GDPR.

[6] European Parliament, Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No . . ./2014 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) - http://www.europarl.europa.eu/sides/getDoc-.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN#BKMD-5.

closed to third parties. However, the proposal received a degree of criticism[7] as the intention behind the icon was not always clear and the inclusion of icons could serve to confuse individuals further.

As mentioned, the introduction of these enhanced information provisions means that controllers should consider reviewing and amending existing notices and privacy policies to ensure compliance with these new prescriptive information requirements. Notices and policies must inform data subjects clearly and concisely and be adapted to the audience. For example, where the information is addressed to a child, such policies should be drafted in such a way so as to be easily understood by children.[8] In particular, the right to object to processing and direct marketing based on legitimate interests should be presented clearly and separately from other information.[9]

B. Subject Access Right

1. Summary of Right

Article 15 of the GDPR grants individuals the right to request access to their personal data being processed by the controller. This right of subject access, which also exists under the Data Protection Directive, requires controllers, in addition to providing a copy of the data subject's personal data, to disclose the following information to the data subject:

(i) the purposes of the processing;
(ii) the categories of personal data processed;
(iii) the recipients of the personal data;
(iv) the retention period or the criteria used to determine the retention period;
(v) the existence of the other data subject rights as well as the right to lodge a complaint with the DPA;
(vi) the source of the personal data where this is not collected from the data subject; and
(vii) the existence of automated decision-making, including profiling as well as ''meaningful information about the logic involved . . . the significance and the envisaged consequences . . . for the data subject.''[10]

The data subject should also be informed of the appropriate safeguards implemented where personal data is transferred outside of the EEA.

2. Compliance with Request

Article 12(3) of the GDPR requires a controller to respond to a subject access request without undue delay and, at the latest, within one month of receipt of the request, although this deadline can be extended for up to an additional two months where there are numerous requests or the request made is complex, provided the data subject is informed of the extension within the original one-month deadline. Controllers should, to the extent one does not already exist, put in place a process to deal with requests and, in particular, verify the identity of requestors in order to comply within the statutory deadlines. Indeed, Recital 59 and Article 12 further require that controllers implement ''modalities'' to facilitate the exercise of data subject rights. This likely requires controllers to put in place systems such as user interfaces that respond to data subject requests. Controllers may consider developing template responses where they receive large volumes of requests.

Unlike under the Data Protection Directive, where a fee could be charged by the controller for responding to a subject access request, Article 12(5) of the GDPR states that a ''reasonable fee'' can only be incurred where requests are ''manifestly unfounded or excessive, in particular because of their repetitive character'' and the onus is on the controller to demonstrate this character.[11] Where a data subject makes the request in electronic form, the controller should respond in electronic form where possible, unless otherwise requested by the data subject.[12] Controllers may want to consider converting existing paper records to electronic format in order to facilitate the requirement to respond electronically.

3. Exemptions

Article 12(2) of the GDPR states that a controller may refuse to respond to a subject access request only where the controller can demonstrate that is it not in a position to identify the data subject. Where a controller has reasonable doubts concerning the identity of the data subject, it can request additional information in order to satisfy its concerns.[13] Where the controller processes a large quantity of information about the data subject, the controller may ask the data subject to specify which information or which processing activities are requested.[14]

C. Right to Erasure

1. The Concept

Article 17 of the GDPR introduces a statutory right for individuals to have their personal data erased without undue delay where:

(i) the data is no longer necessary for the original purpose;
(ii) the consent for the processing is withdrawn and there is no other legal basis for the processing;
(iii) the data subject objects to the processing pursuant to Article 21 (see Section III.E., below);
(iv) the processing is unlawful;
(v) the processing is not in compliance with EU or Member State law; or
(vi) the data has been collected based on the consent of a child's legal guardian in relation to the offering of information society services directly to a child below the age of 16 (see Section II.C.).

Recital 65 of the GDPR stresses the importance of this right where the data subject is a child who has given consent to

[7] *See* http://kau.diva-portal.org/smash/record.jsf?pid=diva2%3A720798&dswid=7857.
[8] Article 12(1) of the GDPR.
[9] Article 21(4) of the GDPR.
[10] Article 15(1) of the GDPR.
[11] Article 12(5) of the GDPR.
[12] Article 12(3) of the GDPR.
[13] Article 12(6) of the GDPR.
[14] Recital 63 of the GDPR.

processing ''and is not fully aware of the risks involved by the processing,''[15] and the data subject later wants to remove such information.

Where the controller is required to erase personal data made public, the controller must take ''reasonable steps'' to inform other controllers processing such data to erase any links to, copies of, or replications of the personal data.[16] In determining what is reasonable, consideration should be given to the available technology, the means available to the controller (including technical measures) to inform controllers processing the data, and the cost of implementation.[17]

2. The Right to Be Forgotten and Spanish Google Case

A similar right was recognized under the Data Protection Directive in the 2014 CJEU case of *Google Spain v AEPD*.[18] In that case, the CJEU ruled that in certain circumstances, search engines must remove from their search results links to websites about an individual where the data therein is incomplete or inaccurate, even if the publication itself on those web pages is lawful. This has become known as an individual's ''right to be forgotten.'' This right is based on a data subject's right to rectification, erasure, or blocking of data under Article 12 of the Data Protection Directive where the processing is not compliant with the provisions of the Data Protection Directive, in particular where the personal data is incomplete or inaccurate. As such, assertions that the right to erasure under Article 17 of the GDPR is a fundamentally new right are incorrect, as the Data Protection Directive already includes the principle underpinning such a right.

Following the CJEU's judgment, the Article 29 Working Party published guidelines for DPAs on the implementation of the judgment.[19] In particular, the guidelines included criteria to be adopted by DPAs when deciding whether the refusal by a search engine to de-list is in compliance with EU data protection laws. The criteria include, for example:

(i) whether the data subject plays a role in public life. The CJEU made an exception for de-listing requests from individuals that play such a role, and here the Article 29 Working Party guidance states that the individual's role ''must justify public access to information about them'' and could include politicians, senior public officials, business people, and members of the regulated professions;

(ii) as a general rule, if the individual is a minor at the time the information is published, the de-listing is more likely;

(iii) de-listing is more appropriate where the information is factually inaccurate and where this ''presents an inaccurate, inadequate, or misleading impression of an individual'';

(iv) depending on the facts of the case, information published a long time ago (for example, 15 years ago) will be less relevant and therefore more likely to result in an approved de-listing;

(v) de-listing is more likely to be approved where the search result reveals sensitive personal data to the public; and

(vi) evidence that a search result is causing prejudice to an individual ''would be a strong factor in favour of de-listing.''[20]

While the guidelines issued by the Article 29 Working Party are not legally binding, similar guidelines may be adopted in respect of the new right to erasure under the GDPR.

Importantly, the right to erasure is more expansive under the GDPR: it applies not only to search engine operators but to all controllers. Given that by October 2015, Google had reportedly received over 350,000 removal requests and evaluated more than 1.2 million links for removal, the impact of the right to erasure on controllers is likely to be a significant undertaking, not least because it may prove difficult to reconcile this requirement with technical limitations on the ability to erase all personal data.

3. Exceptions

The right to erasure is subject to a limited number of exceptions, including where the processing is necessary for:

(i) exercising the right of freedom of expression and information;

(ii) for compliance with an EU or Member State legal obligation to which the controller is subject;

(iii) for reasons of public interest in the area of public health;

(iv) for archiving, scientific, or historical research, or statistical purposes; and

(v) for the defense of legal claims.[21]

In the event of a disagreement as to whether the right to erasure applies, Article 18 of the GDPR establishes a procedure pursuant to which the controller must restrict the processing of personal data at the request of the data subject for ''a period enabling the controller to verify the accuracy of the personal data.''[22] Recital 67 of the GDPR states that methods to restrict processing include, for example, temporarily moving the selected data to another system or removing it from a website. Controllers should check whether their systems can in practice comply with this requirement (*i.e.*, to restrict processing and

[15] Recital 65 of the GDPR.

[16] Article 17(2) and Recital 66 of the GDPR.

[17] Article 17(2) and Recital 66 of the GDPR.

[18] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, [2014] ECLI:EU:C:2014:317, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

[19] Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on ''Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González'' C-131/12, 14/EN WP225 - adopted on Nov. 26, 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[20] Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on ''Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González'' C-131/12, 14/EN WP225 - adopted on Nov. 26, 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[21] Article 17(3) of the GDPR.

[22] Article 18(1)(a) of the GDPR.

mark such data as ''restricted'') and make any necessary amendments to facilitate compliance.

D. Data Portability

1. Summary of the Right

Where personal data is processed in a machine-readable, structured, and commonly-used format, and the processing of the personal data is based on consent or on the performance of a contract with the individual, the data subject has the right pursuant to Article 20 of the GDPR to receive such personal data or to require that such personal data be transferred from one controller to another without hindrance. This right to data portability would, for example, permit a social media user to ask his social media provider to transfer his personal data directly to a competitor rather than having him download the data himself and upload it onto the competitor's platform.

The EDPS has questioned why the right to data portability is limited to the processing of personal data based on consent or on the performance of a contract.[23]

Logically speaking, however, consent and performance of a contract are the only legal grounds where there is a direct relationship between the controller and the data subject.

2. The Right in Practice

The right to data portability has been described as one of the most controversial provisions in the GDPR. Indeed, during negotiations, many Member States questioned whether the right would fit better in consumer or competition legislation, especially given the concerns that the transfer of data in this way may raise issues from a proprietary and/or intellectual property perspective (*i.e.*, the risk that trade secrets, confidential information, or intellectual property of the original controller could be infringed). For example, cloud providers often use proprietary data formats that would limit the ease at which such data could be transferred to an alternative provider. Concerns were also raised over the impact such a right could have on ''new ideas, innovation and competition'' by the UK's Department of Business, Innovation.[24]

In addition, from a purely commercial perspective, mandating controllers to transfer personal data to another controller where, for example, the data subject is not subject to a ''lock-in'' of his data, may subject the controller to disproportionate costs and effort. Likewise, the life sciences industry is concerned that such a right may impact, for example, ongoing clinical research or continuity of services.

An additional practical concern is the interoperability of systems and databases. However, it is acknowledged that the right to transfer personal data from one controller to another is subject to where this is ''technically feasible,'' and Recital 68 of the GDPR states that there is no obligation for controllers to adopt compatible systems. Based on comments from the UK's ICO that controllers may seek to circumvent the requirement where data is not in a ''commonly-used format,''[25] Recital 68 may be intended to address this in turn, by requiring controllers to convert the data to a ''commonly-used format'' where ''technically feasible.'' However, Recital 68 further states that controllers should be encouraged to ''develop interoperable formats that enable data portability.''[26] Unfortunately, not all systems are interoperable, so the question remains: to what extent do companies need to facilitate a transfer of this nature, and what happens, for example, where data affects multiple data subjects who cannot agree on the transfer? Currently, there is no guidance addressing these concerns.

E. Right to Object

1. Right to Object to Processing

While the Data Protection Directive requires a data subject to demonstrate compelling legitimate grounds in order to object to processing of his personal data, Article 21 of the GDPR reverses the burden and permits a data subject to object to processing at any time where the processing is based on either the public interest ground or the legitimate interest of the controller. If the controller wants to continue processing, it must demonstrate compelling legitimate grounds that override the interests of the data subject. As such, this is not an absolute right, and if the controller's legitimate interests outweigh those of the data subject, then the controller is not required to comply with the objection and cease processing. As in the Data Protection Directive, the GDPR permits data subjects to object to processing for direct marketing purposes (*i.e.*, once the data subject objects to the processing of his personal data for direct marketing purposes, the processing must stop), which also includes profiling related to direct marketing.

Data subjects are also given the right to object where their personal data is processed for scientific and historical research purposes or for statistical purposes other than where the processing is necessary for the performance of a task carried out for reasons of public interest.[27]

This right to object (other than in respect of statistical or research-based processing) must be explicitly brought to the attention of the data subject at the time of or before the first communication with the data subject, and the information must be presented clearly and separately from any other information.[28] In the context of online services, a data subject must be given the opportunity to exercise the right to object electronically.[29]

---

[23] See ''Opinion of the European Data Protection Supervisor on the data protection reform package,'' p. 25 (7 March 2012), available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN-.pdf.

[24] Baroness Neville-Rolfe, UK's parliamentary under-secretary of state for the Department for Business, Innovation, giving evidence to the UK parliament's EU Internal Market Sub-Committee's inquiry into online platforms on Dec. 15, 2015 - http://www.parliamentlive.tv/Event/Index/03e4655b-f6e9-44e6-b797-a6139c4b9156.

[25] See ICO, ''Proposed new EU General Data Protection Regulation: Article-by-article analysis paper,'' (Feb. 12, 2013), p. 25, available at https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf.

[26] Recital 68 of the GDPR.

[27] Article 21(6) of the GDPR.

[28] Article 21(4) of the GDPR.

[29] Article 21(5) of the GDPR.

2. *Right to Object to Profiling*

a. *Big Data*

The Article 29 Working Party in its *Opinion 03/2013 on purpose limitation* defines ''Big Data'' as ''the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed ... using computer algorithms.''[30]

The expectation of Big Data, as acknowledged by the Commission in its digital strategy, is that it will not only boost growth and jobs ''but also improve the quality of life [for] Europeans''.[31] In its Digital Single Market Strategy Working Document, the Commission further predicts that ''by 2020 more than 16 zettabytes of useful data will exist, which implies an equivalent growth of 236% per year from 2013 to 2020.''[32] The Strategy describes Big Data as ''a catalyst for economic growth, innovation, and digitisation across all economic sectors . . . and for society as a whole.''[33]

A primary means of extracting value from Big Data is by profiling, a concept used widely in both the private and public sectors in legitimate ways that are beneficial to society. For example, in the healthcare sector, profiling is used to support clinical decisions, disease surveillance, and population health management. In the financial sector, for example, profiling is used for the prevention and detection of credit card fraud and to improve risk analysis and pricing.

b. *Profiling*

Article 4(4) of the GDPR defines profiling as the automated processing of personal data in order to evaluate certain personal aspects relating to a natural person. The examples given in Recital 71 of the GDPR are very wide and include analyzing or predicting ''aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability, or behaviour, location, or movements.''[34]

c. *The Concept and the Requirements*

The GDPR introduces new restrictions on controllers carrying out profiling. Article 22 provides that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or that similarly significantly affects an individual other than where necessary for the performance of a contract, authorized by national Member State law, or conducted with the explicit consent of the individual.[35] Recital 71 of the GDPR provides, as examples of decisions based on automated processing, the ''automatic refusal of an online credit application or e-recruiting practices without any human intervention.''[36]

Decisions based solely on profiling sensitive personal data are permitted only in limited circumstances (*i.e.*, with the explicit consent of the data subject or where the profiling is necessary for reasons of substantial public interest). In those circumstances, appropriate safeguards must be implemented.[37]

Article 13 of the GDPR, as discussed above, subjects a controller to additional obligations when engaging in profiling, in particular with regard to the logic involved in the profiling and the consequences of such profiling. In many examples of profiling and in particular where the controller is using personal data from secondary sources, it may be impracticable for a controller to comply with these obligations. In those instances, a controller will likely need to rely on the exemption in Article 14(5)(b), which applies to the extent the provision of such information ''proves impossible or would involve a disproportionate effort.''[38] Controllers engaging in profiling activities should consider how they can implement appropriate mechanisms for transparency and consent in order to continue these activities in compliance with the GDPR.

Article 35(3) of the GDPR requires a privacy impact assessment to be carried out in all instances of profiling. This provision is likely to be significant for controllers engaging in profiling (see Section IV.A.2.b.).

According to Recital 71, to ensure fairness and transparency, all profiling should use ''appropriate mathematical or statistical procedures,'' and technical and organizational measures should be implemented to correct data inaccuracies and minimize the risk of errors.[39] In addition, personal data should be secured in a way that ''prevents, *inter alia*, discriminatory effects on natural persons.''[40]

d. *Big Data in Practice*

A number of EU authorities have issued guidance on the interplay between data protection and Big Data.

Indeed, the EDPS, in *Opinion 7/2015 Meeting the challenges of big data*, states that ''the question is not whether to apply data protection law to big data, but rather how to apply it innovatively in new environments.''[41]

---

[30] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203 00569/13/EN – adopted on April 2, 2013, p. 35, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[31] https://ec.europa.eu/digital-single-market/what-big-data-can-do-you.

[32] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015SC0100.

[33] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52015DC0192.

[34] Recital 71 of the GDPR.

[35] Article 22(2) of the GDPR.

[36] Recital 71 of the GDPR.

[37] Article 22(4) of the GDPR.

[38] Article 14(5)(b) of the GDPR.

[39] Recital 71 of the GDPR.

[40] Recital 71 of the GDPR.

[41] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Nov. 19, 2015, page 4 – available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

In *Opinion 7/2015*, the EDPS sets out ''four essential elements'' that it believes ''responsible and sustainable development of big data must rely on . . .''[42] The four essential elements are:

(i) greater transparency from controllers about how data is processed (*i.e.*, individuals must be given clear information on what data is being used and for what purposes, including the logic used in algorithms to make assumptions);

(ii) a higher degree of control for individuals over how their data is used (for example, the right to erasure);

(iii) data protection designed into procedures and services (for example, anonymization techniques and functional separation with innovative means to inform individuals); and

(iv) more accountable controllers,[43] for which the EDPS flags three key considerations:

a. ''whether any secondary use of data complies with the principle of purpose limitation'';

b. ''whether data initially used in one context can be considered adequate, relevant, and proportionate to be reused in another context''; and

c. ''whether, in the absence of obtaining consent from the individuals, an organisation can rely on its legitimate interest to process any data.''[44]

In terms of national guidance, the UK's ICO issued guidance in 2014 for companies to ensure their Big Data initiatives are compliant with data protection laws.[45] Some of the key points raised in the ICO's guidance are as follows:

- To ensure fair processing, a data protection impact assessment should be carried out. If a risk is identified, the company has the opportunity to identify creative technical solutions to protect individuals' privacy (see Section IV.A.).
- The quality and reliability of data is a potential issue for Big Data analytics, in part because the frequency of data processing increases the risk of inaccuracies, especially where the data has been partially de-identified or anonymized and cannot be reconnected with its original data subject. Potentially negative consequences for the data subject related to inaccurate profiling, discrimination, or prejudicial action are serious risks.
- The purpose limitation principle is a barrier to the development of Big Data analytics, as most secondary uses have not been thought of when the data is first collected. A compatibility assessment should be carried out (see Section IV.A.) and/or consideration given to the possible ''research'' exemption.[46]
- In order to ensure compliance with the data minimization principle (which is the opposite of the objective of Big Data analytics), companies should identify at the outset why they need the particular data and what they expect to learn from its analysis. In terms of data retention, controllers must be able to justify the retention of the data or alternatively to anonymize the data, in turn bringing it out of the scope of the EU data protection laws.
- The ICO considers it too simplistic to say that in general Big Data either increases or decreases information security risk. However, it acknowledges there is a potential for increased risk, but says that this can be mitigated by applying normal security procedures and by the use of Big Data in security analytics.

Businesses should review their current profiling activities and determine if these activities result in decisions that legally affect or significantly affect individuals. Where this is the case, a business should determine if the activities are covered by one of the limited exemptions. If the activities do not fall within the exemptions, they should be modified to ensure compliance with the GDPR.

However, even where the processing is in compliance with the GDPR and/or the privacy-related guidance, there is still the broader ethical debate surrounding Big Data analytics. A number of papers have been published on the ethical considerations pertaining to Big Data analytics, many of which state that Big Data analytics must consider *all* individual interests and human rights (*i.e.*, not just those interests that are privacy-related). For example, Article 5(1) of the GDPR requires that personal data be processed fairly, which, from a data privacy perspective, generally requires transparency. However, from an ethical perspective, the concept of fairness would include ensuring a data subject's right to privacy, while also balancing that right with integrity. Companies engaged in Big Data analytics, therefore, need to consider the broader ethical impact of their processing

[42] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Nov. 19, 2015, page 4 – available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

[43] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Nov. 19, 2015, page 4 – available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

[44] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Nov. 19, 2015, pages 15 and 16 – available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

[45] UK's Information Commissioner's Office, Big data and data protection, 2014 - https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf.

[46] Article 5(1)(b) of the GDPR states that ''further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.'' Article 89(1) of the GDPR provides that such processing shall be subject to appropriate safeguards for the rights and freedoms of the data subjects. In particular, the safeguards shall ensure data minimization and may include pseudonymization. However, where further processing can be fulfilled using anonymous data, then anonymous data should be used.

activities. Indeed, the information technology research and advisory company Gartner, Inc. predicts that by 2018, half of business ethics violations will occur through improper use of Big Data analytics.[47]

---

[47] *Gartner Says, By 2018, Half of Business Ethics Violations Will Occur Through Improper Use of Big Data Analytics*, Gartner - http://www.gartner.com/newsroom/id/3144217.

