General Data Protection Regulation

From Wikipedia, the free encyclopedia

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC)[2] from 1995. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments and is thus directly binding and applicable.[3]

Regulation (EU) 2016/679

European Union regulation	
Title	Regulation 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)
Made by	European Parliament & Council
Journal reference	L119, 4/5/2016, p. 1–88 (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)
History	
Date made	27 April 2016
Implementation date	25 May 2018
Preparative texts	
Commission proposal	COM/2012/010 final - 2012/0010 (COD)
Other legislation	
Replaces	Data Protection Directive
Current legislation	

Contents

Summary

"The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover."[4]

Content

The proposal for the European Data Protection Regulation contains the following key requirements:[5][6]

Scope

The regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU. Furthermore the Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents. According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."[7] The regulation does not apply to the processing of personal data for national security activities or law enforcement; however, the data protection reform package includes a separate Data Protection Directive for the police and criminal justice sector that provides robust rules on personal data exchanges at national, European and international level.

Single set of rules and one-stop shop

A single set of rules will apply to all EU member states. Each member state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. SAs in each member state will cooperate with other SAs, providing mutual assistance and organising joint operations. Where a business has multiple establishments in the EU, it will have a single SA as its "lead authority", based on the location of its "main establishment" (i.e., the place where the main processing activities take place). The lead authority will act as a "one-stop shop" to supervise all the processing activities of that business throughout the EU[8][9] (Articles 46–55 of the GDPR). A European Data Protection Board (EDPB) will coordinate the SAs. EDPB will replace Article 29 Working Party.

There are exceptions for data processed in an employment context and data processed for the purposes of national security, that still might be subject to individual country regulations (Articles 2(2)(a) and 82 of the GDPR).

Responsibility and accountability

The notice requirements remain and are expanded. They must include the retention time for personal data and contact information for data controller and data protection officer has to be provided.

Automated individual decision-making, including profiling (Article 22) is made contestable. Citizens now have the right to question and fight decisions that affect them that have been made on a purely algorithmic basis. Many media outlets have commented on the introduction of a "right to explanation" of algorithmic decisions[10][11], but legal scholars have since argued that the existence of such a right is highly unclear without judicial test, and limited at best.[12][13]

In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures which meet the principles of data protection by design and data protection by default. Privacy by Design and by Default (Article 25) require that data protection measures are designed into the development of business processes for products and services. Such measures include pseudonymising personal data, by the controller, as soon as possible (Recital 78).

It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller. (Recital 74).

Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks. Data Protection Officers (Articles 37–39) are to ensure compliance within organizations.

They have to be appointed:

- for all public authorities, except for courts acting in their judicial capacity
- if the core activities of the controller or the processor consist of
  - processing **operations** which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
  - processing on a large **scale** of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10[14]

Consent

Valid consent must be explicit for data collected and the purposes data is used for (Article 7; defined in Article 4). Consent for children[15] must be given by the child's parent or custodian, and verifiable (Article 8). Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.[16]

Data Protection Officer

Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, or where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations. The appointment of a DPO within a large organization will be a challenge for the Board as well as for the individual concerned. There are a myriad of governance and human factor issues that organizations and companies will need to address given the scope and nature of the appointment. In addition, the post holder will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organization that employs them, effectively as a "mini-regulator".

More details on the function and the role of Data Protection Officer were given on 13 December 2016 with a guideline document.[17]

Pseudonymisation

The GDPR refers to pseudonymisation as a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information. An example of pseudonymisation is encryption, which renders the original data unintelligible and the process cannot be reversed without access to the correct decryption key. The GDPR requires that this additional information (such as the decryption key) be kept separately from the pseudonymised data. Pseudonymisation is recommended to reduce the risks to the concerned data subjects and also help controllers and processors to meet their data-protection obligations (Recital 28).

Although the GDPR encourages the use of pseudonymisation to "reduce risks to the data subjects," (Recital 28) pseudonymised data is still considered personal data (Recital 26) and therefore remains covered by the GDPR.

Data breaches

Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority without undue delay. The reporting of a data breach is not subject to any *de minimis* standard and must be reported to the Supervisory Authority within 72 hours of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (Article 34). In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach (Article 33).

However, the data processor or controller do not have to notify the data subjects if anonymized data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudonymisation techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach (Article 34).

Sanctions

The following sanctions can be imposed:

- a warning in writing in cases of first and non-intentional non-compliance
- regular periodic data protection audits
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4[18])
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 5 & 6[18])

Right to erasure

A *right to be forgotten* was replaced by a more limited *right to erasure* in the version of the GDPR adopted by the European Parliament in March 2014.[19][20] Article 17 provides that the data subject has the right to request erasure of personal data related to them on any one of a number of grounds including non-compliance with article 6.1 (lawfulness) that includes a case (f) where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (see also *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*).

Data portability

A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. Data that has been sufficiently anonymised is excluded, but data that has only been de-identified but remains possible to link to the individual in question, such as by him or her providing the relevant identifier, is not.[21] Both data that has been 'provided' by the data subject, and data that has been 'observed' — such as about their behaviour — is within scope. In addition, the data must be provided by the controller in a structured and commonly used Open Standard electronic format. The right to data portability is provided by Article 20 of the GDPR.[6] Legal experts see in the final version of this measure a "new right" created that "reaches beyond the scope of data portability between two controllers as stipulated in Article 18".[22] (Note that the Article number was updated to Article 20 in the final release version. The quotation was accurate at the time.)

Data protection by Design and by Default

Data protection by Design and by Default (Article 25) requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default, and that technical and procedural measures should be taken care by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

A report[23] by ENISA (the European Union Agency for Network and Information Security) elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

Records of processing activities

Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request.[24] (article 30).

Timeline

The proposal[9] for GDPR was released on 25 January 2012 and the EU Council aimed for formal adoption in early 2016.[25]

The schedule is

- 21 October 2013: European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) had its orientation vote.
- 15 December 2015: Negotiations between European Parliament, Council and Commission (Trilogue) have resulted in a joint proposal.
- 17 December 2015: European Parliament's LIBE committee voted positively on the outcome of the negotiations between the three parties.
- 8 April 2016: Adoption by the Council of the European Union.[26]
- 14 April 2016: Adoption by the European Parliament.[27]
- The regulation entered into force 20 days after its publication in the EU Official Journal on 4 May 2016.[28] Its provisions will be directly applicable in all member states two years after this date.
- It shall apply from 25 May 2018.[28]

Discussion and challenges

The proposal for the new regulation gave rise to many discussions and controversy. Thousands of amendments were proposed.[29] The single set of rules and the removal of administrative requirements were supposed to save money. But critics pointed to these issues

- The requirement to have a Data Protection Officer (DPO) is new for many EU countries and criticized by some for its administrative burden.
- The GDPR was developed with a focus on social networks and cloud providers, but did not consider requirements for handling employee data sufficiently.[30]
- Data portability is not seen as a key aspect for data protection, but more a functional requirement for social networks and cloud providers.
- Language and staffing challenges for the Data Protection Authorities (DPA):
  - Non-European companies might prefer the Irish DPA (or the UK while it remains in the EU) because of the English language. This will require extensive resources in those countries.
  - EU citizens no longer have a single DPA to contact for their concerns, but have to deal with the DPA chosen by the company involved. Communication problems due to foreign languages have to be expected.
- The new regulation conflicts with other non-European laws and regulations and practices (e.g. surveillance by governments). Companies in such countries should no longer be considered acceptable for processing EU personal data. See EU-US Privacy Shield.
- The biggest challenge might be the implementation of the GDPR in practice:
  - The implementation of the EU GDPR will require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force (especially non-European companies handling EU personal data).
  - There is already a lack of privacy experts and knowledge as of today and new requirements might worsen the situation. Therefore education in data protection and privacy will be a critical factor for the success of the GDPR.
  - The European Commission and DPAs have to provide sufficient resources and power to enforce the implementation and a unique level of data protection has to be agreed upon by all European DPAs since a different interpretation of the regulation might still lead to different levels of privacy.
  - Europe's international trade policy is not yet in line with the GDPR.[31]

See also

- National data protection authorities
- European Data Protection Board successor of Article 29 Data Protection Working Party

References

1. Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex.", 201 pages, 11 June 2015, PDF, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
2. "Directive 95/46/EC" (http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046)
3. Blackmer, W.S. (5 May 2016). "GDPR: Getting Ready for the New EU General Data Protection Regulation" (http://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/). *Information Law Group*. InfoLawGroup LLP. Retrieved 22 June 2016.
4. "New draft European data protection regime" (http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227). m law group. Retrieved 3 January 2013.
5. "Inofficial consolidated version GDPR" (http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf). Rapporteur Jan Philipp Albrecht. Retrieved 9 December 2013.
6. Proposal for the EU General Data Protection Regulation (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf). European Commission. 25 January 2012. Retrieved 3 January 2013.
7. European Commission's press release announcing the proposed comprehensive reform of data protection rules (http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en). 25 January 2012. Retrieved 3 January 2013.
8. The Proposed EU General Data Protection Regulation. A guide for in-house lawyers, Hunton & Williams LLP, June 2015, p. 14
9. "GDPR proposal" (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)
10. editor, Ian Sample Science (2017-01-27). "AI watchdog needed to regulate automated decision-making, say experts" (https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions). *The Guardian*. ISSN 0261-3077 (https://www.worldcat.org/issn/0261-3077). Retrieved 2017-07-15.
11. "EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence" (http://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm). *www.techzone360.com*. Retrieved 2017-07-15.
12. Wachter, Sandra; Mittelstadt, Brent; Floridi, Luciano (2016-12-28). "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (https://papers.ssrn.com/abstract=2903469) – via SSRN.
13. Edwards, Lilian; Veale, Michael (2017-05-23). "Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking For" (https://papers.ssrn.com/abstract=2972855) – via SSRN.
14. "EUR-Lex – Art. 37" (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679). *eur-lex.europa.eu*. Retrieved 2017-01-23.
15. Regulation article 8 (1):"For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian."
16. "How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide" (https://www.privacyassociation.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf). Judy Schmitt, Florian Stahl. 11 October 2012. Retrieved 3 January 2013.
17. "Guidelines on Data Protection Officers" (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf) (PDF). Retrieved 23 January 2017.
18. Article 83, GDPR (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1)
19. Baldry, Tony; Hyams, Oliver. "The Right to Be Forgotten" (http://1essexcourt.wordpress.com/2014/05/15/the-right-to-be-forgotten/). 1 Essex Court.
20. "European Parliament legislative resolution of 12 March 2014 on the 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)" (http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN). European Parliament.
21. Article 29 Working Party (2017). *Guidelines on the right to data portability* (http://ec.europa.eu/newsroom/document.cfm?doc_id=44099). European Commission.
22. "The Final European Union General Data Protection Regulation, by Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot and Sára G. Hoffman, Section II, 4" (http://www.bna.com/final-european-union-n57982067329/#!). Bloomberg BNA. 12 February 2016.
23. "Privacy and Data Protection by Design — ENISA" (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design). *www.enisa.europa.eu*. Retrieved 2017-04-04.
24. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (article 30)" (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3265-1-1).
25. The EU General Data Protection Regulation Timeline, Allen & Overy (http://www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx)
26. Data protection reform: Council adopts position at first reading (http://www.consilium.europa.eu/en/press/press-releases/2016/04/08-data-protection-reform-first-reading/)
27. Data protection reform – Parliament approves new rules fit for the digital era (http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era)
28. EU Official Journal issue L 119 (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN)
29. Overview of amendments (http://lobbyplag.eu/map). LobbyPlag. Retrieved 23 July 2013.
30. Expert tips: Get your business ready for GDPR (https://tresorit.com/blog/expert-tips-business-gdpr-ready/). Regina Mühlich. Retrieved 9 August 2016.
31. "Irion, K., S. Yakovleva, M. Bartl: Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements" (http://ivir.nl/publicaties/download/1807). Institute for Information Law (IViR), University of Amsterdam. 22 September 2016.

External links

- Regulation (EU) 2016/679 of the European Parliament and of the Council (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679) 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)
- EU Data Protection page (http://ec.europa.eu/justice/data-protection/index_en.htm)
- General Data Protection Regulation, final version dated 27 April 2016 (http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)
- Procedure 2012/0011/COD (http://eur-lex.europa.eu/procedure/EN/201286), EUR-Lex
- 2012/0011(COD) – Personal data protection: processing and free movement of data (General Data Protection Regulation) (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29), European Parliament
- How to prepare for proposed EU data protection regulation (Computerweekly) (http://www.computerweekly.com/opinion/Proposed-EU-Data-Protection-Regulation-what-should-companies-be-thinking-about)