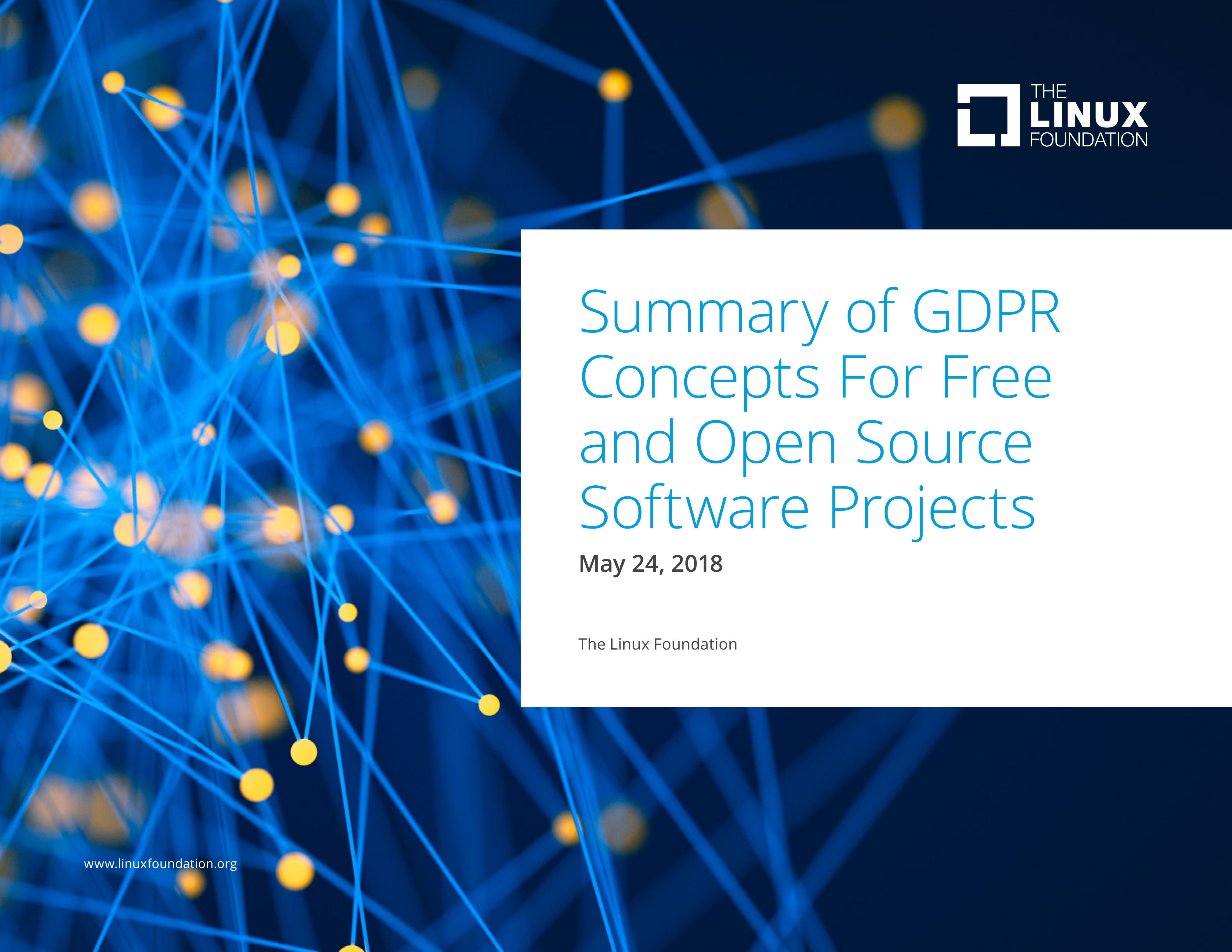

THE LINUX FOUNDATION

Summary of GDPR Concepts For Free and Open Source Software Projects

May 24, 2018

The Linux Foundation

www.linuxfoundation.org

Summary

This summary provides basic details about the General Data Protection Regulation (GDPR). It is intended to address some of the high-level concepts and topics regarding compliance with the GDPR.

Please note that this is intended only as a helpful summary and guide and is not legal advice. You should consult with your own legal counsel regarding any questions relating to GDPR compliance for yourself and your projects.

What is the GDPR

The GDPR is the European Union's General Data Protection Regulation. It is an 88-page document that describes the principles and obligations that must be followed when collecting and processing personal data of EU residents. While it is an EU regulation, it applies to any organization in the world that processes data on EU residents. It was enacted by the European Parliament in April 2016. It becomes effective on May 25, 2018. The GDPR's full text can be read *here*[1].

Why was the GDPR enacted?

The GDPR was enacted to address and modify a number of factors in previous data protection frameworks, particularly in light of changes in technology over time. These goals included:

- *Imposing stricter and broader requirements to protect personal data.* The EU's previous data privacy framework, the Data Protection Directive (DPD), became viewed as insufficiently protective of individuals' data. This was especially true in light of increasing concerns about security breaches, governmental surveillance of individuals, and widespread sharing and misuse of personal data.
- *Creating a single set of requirements.* Previously, under the DPD, each country in the EU had to pass its own rules implementing the DPD in their own laws. This led to over 25 differing national sets of laws to comply with, which varied greatly in scope. The GDPR, by contrast, is a single regulation that harmonizes the rules across EU members.
- *Clarifying individuals' rights to access and control their personal data.* The GDPR explicitly codifies several categories of rights given to EU residents regarding their own personal data. These are described in greater detail below.
- *Enabling significant penalties for non-compliance.* The DPD was seen as insufficient to motivate some companies to comply. The GDPR, by contrast, enables data regulators to punish non-compliance with significant fines of up to the greater of 20 million euros or 4% of annual global revenue.

[1] *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679*

When do I need to think about the GDPR?

Communities should consider the GDPR any time they are collecting, storing, using or transferring personal data.

What is “personal data”?

Under the GDPR, **“personal data”** is any information that relates to an identified or identifiable natural person. The person it relates to is called the **“data subject.”**

“Personal data” is an extremely broad term. It includes:

- information that can identify someone directly, alone or in context - sometimes called “personally identifiable information” (e.g. a national identification number; a name; a date of birth; an email address)
- information that can identify someone indirectly (e.g. job title + company - “Director of Widgets at Company ABC”)
- information that can be linked to that person (e.g. postings, order details, banking details, medical information, IP addresses, ...)

What is “sensitive data” or “special data”?

Certain categories of data are considered **“sensitive data”** or **“special data”**, and are subject to higher thresholds of permission to be allowed to collect or process them. These include in particular:

- racial or ethnic origin
- political opinions, religious or philosophical beliefs, or trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person’s sex life or sexual orientation

What does it mean to “process” personal data?

Personal data is **“processed”** any time an operation is performed on it. This includes collecting, storing, viewing, transmitting, and deleting it, whether or not by automated means.

What are the GDPR’s “principles” on processing personal data?

The GDPR defines seven primary **principles** for processing personal data. These are:

- *Lawfulness, Fairness and Transparency.* Process personal data in a way that is legal, fair and transparent to the data subject.
- *Purpose Limitation.* Only process personal data in ways that are compatible with the legitimate purposes for which it was collected.
- *Data Minimisation.* Limit the personal data you collect to what’s adequate for those purposes.

- *Accuracy.* Keep personal data accurate and up to date, and take every reasonable step to erase or rectify inaccurate data.
- *Storage Limitation.* Store personal data in a form which permits identification for no longer than needed for the purposes for which it was collected.
- *Integrity and Confidentiality.* Process personal data in a way that ensures appropriate security.
- *Accountability.* A controller of personal data is responsible for the above principles, and for demonstrating its compliance with them.

What does it mean for processing to be “lawful”?

The GDPR also defines several different categories of purposes that can count as **lawful**. In order to process personal data, the reasons for processing it must fall into at least one of these categories. A processing purpose can have more than one lawful basis (and it is best when it does).

Some of the relevant lawful bases that may permit processing personal data are:

- *Compliance with Law.* Personal data can be processed if it’s necessary for compliance with a legal obligation.
    - Example: When required by law to maintain personal data contained in accounting records for a certain length of time, then that processing is most likely “lawful” under the GDPR.
- *Performing a Contract with the Data Subject.* Personal data can be processed if it’s necessary to perform a contract that is with that data subject. (Note that this likely does not apply to a contract with somebody other than the data subject, such as their employer.)
    - Example: If an individual signs a contract (e.g. when registering to attend a conference), then it is most likely “lawful” under the GDPR to process personal data as needed to perform that contract (e.g. to enable their attendance at the conference).
- *Legitimate Business Interests.* Personal data can be processed if doing so is consistent with “legitimate interests,” unless overridden by the data subject’s interests to the contrary.
    - This can be a more ambiguous concept. The GDPR says that determining the balance of interests needs “careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.”
    - Example: When an individual contributes source code to an open source project, some personal data (such as name and email address) is typically included in that “commit.” That personal data is made publicly available within the project repository. This processing is most likely “lawful” under the GDPR as a legitimate interest, because on balance (1) supporting open source project development is a key purpose for which the data was contributed, and (2) it was clear to the data subject when they made the contribution that

    their contribution and data would have been made public. For instance, sign-offs under the *Developer Certificate of Origin*, section (d), include an attestation regarding personal information contained in the record of the contribution.

    - Note that other lawful bases - in addition to legitimate interests - may also apply to “commit” data.

- *Consent.* Personal data can be processed if the data subject gives their consent.
    - However, for consent to be valid under the GDPR, it must be “specific” and “informed” (e.g., it should include a specific description of what data is being collected, and how it will be used); it requires a “clear affirmative action” by the data subject (e.g., requiring the participant to check a checkbox, and not having it pre-checked); and it must be freely revocable (e.g., the data subject must be able to withdraw consent at any time).
    - Even if a project gets consent, it may also want to evaluate whether it can rely on one or more of the other lawful bases described above, in particular if the data is necessary to be retained.

What are “GDPR requests”? What rights do individuals have under the GDPR?

Six articles in the GDPR lay out specific rights given to individuals regarding their personal data. This gives EU residents the right to contact a data controller and request that it take certain actions (“GDPR requests”). The types of requests described in the GDPR include the following:

- *Right of Access (Art. 15).* Data subjects can ask whether their personal data is being processed. If it is, they can receive “access” to the data (e.g., a copy or screenshot of it) and information regarding the processing.
- *Right to Rectification (Art. 16).* Data subjects can have inaccurate data updated and corrected.
- *Right to Erasure (a.k.a “Right to be Forgotten”) (Art. 17).* In certain circumstances, data subjects can have their personal data erased.
- *Right to Restriction of Processing (Art. 18).* In certain circumstances, data subjects can restrict processing of their personal data. It can still be stored (unless a “Right to Erasure” request was also made).
- *Right to Data Portability (Art. 20).* In certain circumstances, data subjects can have their personal data exported (e.g., provided to the data subject or a third party in a structured, commonly used and machine-readable format).
- *Right to Object (Art. 21).* In certain circumstances (particularly for direct marketing and profiling purposes), data subjects can object to having their personal data processed.

For each of these rights, there are nuances and exclusions; these are generally not absolute rights in all circumstances.

What are “controllers” and “processors”?

These are two different ways to describe a company’s role in processing a particular set of personal data. A **“controller”** is the company who determines the purpose and means of processing. A **“processor”** is a third party that processes it on a controller’s behalf. For example:

- When a company collects HR data about their employees, they are a controller of that data.
- When a company sends some HR data to a third-party service provider to process payroll, the third party service provider is a processor of that data.

This distinction is particularly relevant when personal data will be transferred to or from a third party.

What are Data Processing Addendums (DPAs)?

“DPA” is a commonly-used acronym for various names of agreements (sometimes called “Data Processing Addendums” or “Data Protection Agreements”). These are sets of contract clauses that spell out the parties’ responsibilities for protecting personal data. They may be standalone or may be attached to a separate contract between the parties.

DPAs are important because they establish the legal framework that allows two parties, under the GDPR, to transfer personal data between themselves. There are typically different types of DPAs depending on whether the parties are joint controllers or whether one is a processor for the other.

DPAs can be quite short (just a couple of pages) or can be extremely long, including many details about security protections and organizational policies.

What is “Privacy Shield”?

If personal data is being transferred outside of the EU, the GDPR requires that “appropriate safeguards” be put in place. One mechanism for US organizations to meet these safeguards is to participate in the *Privacy Shield Framework*[2]. This is a self-certification mechanism established between the US and the EU, where companies agree to take on a set of enforceable commitments regarding protection of personal data.

What are “Standard Contractual Clauses” or “Model Clauses”?

Standard Contractual Clauses, sometimes also called “Model Clauses,” are another mechanism that is considered to provide appropriate safeguards for transfers out of the EU. They can be signed between two parties for use with transfers of data between those two specific parties. They are sets of contract terms that were previously drafted and approved by the EU, and cannot be modified.

There are typically different versions of Standard Contractual Clauses depending on whether the parties are joint controllers, or whether one is a processor for the other. Standard Contractual Clauses may be incorporated into “long-form” DPAs.

[2] *https://www.privacyshield.gov/*

What is “profiling”?

Under the GDPR, “profiling” is any form of automated processing that involves using personal data to evaluate aspects of that person. An action would particularly be considered “profiling” when used to analyze or predict a person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Profiling will usually require getting explicit consent from the individual, which means also that the individual will be able to withdraw that consent at any time. Therefore, profiling activities will typically require a greater degree of review and protections for the applicable personal data.

THE LINUX FOUNDATION

The Linux Foundation promotes, protects and standardizes Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about The Linux Foundation or our other initiatives please visit us at **www.linuxfoundation.org**