BRIEF

THE GDPR

For Small and Mid-Size NGOs

Key Principles and Essential Steps to be Taken Now

Legal Disclaimer: *ADF International makes data protection and data privacy rights a priority. In particular, we have employed considerable efforts to analyze and, where necessary, revise our policies and IT systems to ensure GDPR compliance. This brief is for general information purposes only. It points out key aspects of the new regulation and encourages you to actively engage and undertake the necessary steps that are right for your organization. It does not constitute legal advice, nor does it create a lawyer-client relationship. ADF International cannot and does not assume any responsibility or liability whatsoever for the GDPR compliance of you and/or your organization. Data protection is a complex matter and we recommend that you contact your legal advisor to address any specific concerns.*

As of late, have you received an email from the issuer of your favourite newsletter, asking you to renew your subscription in order to continue receiving it? Have you been contacted by your bank or any software company whose product you are using, about changes to their general terms, related to new data protection laws? You might have heard that new technical safeguards are advisable for anyone dealing with personal data, and that any breach of the 'GDPR' may entail a fine of up to 20 Million Euro. What is this new regulation and how does it affect you?

What is the GDPR?

In a world that is increasingly shaped by the exchange of information and data processing, the protection of personal data increases in relevance literally every day. Alongside technical development, countries have been implementing data protection laws since the early 1970s. While technological innovation has accelerated, legal developments have often lagged behind. As regulation came into effect, domestic and international courts over time have further developed individuals' rights in relation to personal data and privacy. Still, the level of protection in each country varies according to national standards.

After several years of consultations and drafting, the European Union adopted the General Data Protection Regulation (GDPR) in 2016.[1] The GDPR replaces the Data Protection Directive 95/46/EC and harmonizes the 28 member states' regulation by setting a common standard for processing the personal data of anyone in the EU worldwide.[2] A two-year grace period, intended to give individuals, businesses, and NGOs subject to the

1 GDPR in official EU languages: http://data.europa.eu/eli/reg/2016/679/oj, more information on EU data protection law: https://ec.europa.eu/info/law/law-topic/data-protection_en.

2 The material scope of the GDPR is tied to the scope of EU jurisdiction. Furthermore, member states may set stricter standards. Consequently, it is important to also monitor the national law of countries in which your organization is based or in which you operate.

new regulation time to get ready, will expire on 25 May 2018. From that date on, the GDPR will be fully enforceable. This means that compliance must be achieved by that point with significant penalties for non-compliance.

- The European Commission has also proposed a revision of the e-Privacy regulation, dealing with, inter alia, direct marketing via email.[3] Originally, the e-Privacy regulation was intended to come into effect at the same time as the GDPR. However, it has been delayed and it is currently unknown when it will be enacted.

Key terminology used throughout the GDPR

1. **Data subject:** A natural person.
2. **Personal data:** Any information relating to a data subject who is or can be directly or indirectly identified by one or more identifiers such as name, identification number, location data or online identifier, bank account, credit card number, etc. (note that the list is not exhaustive!).
3. **Sensitive personal data:** 'Special categories of personal data' (Article 9 GDPR), including genetic and biometric data, information on ethnic origin, health status, religious belief, sexual orientation of a person, etc.
4. **Controller:** A controller determines the purposes and means of processing personal data.
   - Likely, this is you or your organization.
5. **Processor:** A processor is responsible for processing personal data on behalf of a controller.
   - These are your service providers (cloud computing services, lettershops, event organizers, travel agents, etc.)
6. **Processing:** This is practically anything you can do with personal data, including (but not limited to) collection, storage, alteration, consultation, dissemination, combination, erasure. It does not matter whether this is done electronically or on paper.

A word on the territorial applicability of the law

The GDPR always applies to EU-established controllers and processors. However, it also applies regardless of the location of a controller or processor whenever personal data of data subjects then physically present in the EU is processed. This means that even if your organization has no presence in the EU, the GDPR is applicable if and to the extent you process personal data of data subjects who are in the EU at that time.

- Regardless of Brexit, from 25 May 2018 onwards, the GDPR will also be fully applicable to organizations established in the UK. For the time after Brexit takes effect in March 2019, a new Data Protection Bill that will enshrine the basics of GDPR in British law has been proposed. The details remain to be seen.

Consequently, whenever such personal data leaves the EU, special rules for transfer to a third country must be observed. Among other things, data subjects need to be informed of the intention to transfer personal data outside the EU and safeguards must be in place to achieve an adequate level of protection (see Art. 13 and Art. 44 seqq. GDPR).

- It is highly likely that a 'transfer to a third country' happens when personal data is processed in the 'cloud', unless it is certain that the servers of the cloud provider are physically located in the EU, and on its way there and back, data does leave the EU. Popular applications such as email, instant messaging, office programs and backup, etc., should be carefully examined in light of the GDPR given that many service providers are physically located in the United States and elsewhere.

Structure and core obligations under GDPR

The GDPR is built on the individual data subject's rights, and distinct rights are set forth by the regulation (see Art. 12 seqq.), namely:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

3 Draft 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), further information here: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

To safeguard these rights, GDPR, Art. 5 seqq. sets out a number of principles to be applied when processing personal data, namely:

1. **Principle of lawfulness, fairness and transparency:** There must be a legal basis for any processing activity, the options are prescribed in Art. 6 GDPR.
   - ⊕ 'Consent' of the data subject (oftentimes documented through an electronic opt-in procedure) is one of the lawful bases mentioned in Art. 6 GDPR. However, there are other options: One is the fulfillment of a contract. Another one of them is 'legitimate interest'. The latter requires a balancing test between your legitimate interests to process and the data subjects' rights. Such an exercise should be carried out for each processing activity and be documented, when choosing this as a lawful basis for processing activities.
2. **Principle of purpose limitation:** Data is always collected for a specified purpose and as a general rule cannot be used for other purposes.
3. **Principle of data minimization:** Collect and store only personal data you need for a specific purpose.
4. **Principle of accuracy:** Personal data must be kept up to date.
5. **Principle of storage limitation:** The possibility to identify a data subject based on personal data must be limited in time.
6. **Principle of integrity and confidentiality:** Unauthorized access must be excluded.
7. **Principle of accountability:** The controller is responsible for all processing activities (including a processor's activities) and must be able to demonstrate compliance with the abovementioned principles.

Consequently, all of your systems, software solutions and procedures should be designed to maximize data protection and, when there is a choice, the most secure and privacy friendly option must be the default option.

The GDPR obliges you to inform data subjects beforehand of the lawful basis, the purpose of data collection, the duration of storage and other facts as set forth in Articles 13 and 14 GDPR.

⊕ Apart from individually relaying this to each and every data subject upon each individual processing operation, a general privacy policy openly available on your website may be a suitable way to fulfil this obligation.

Where your lawful basis for data processing is consent, you must obtain it through a wilful act of the data subject ('opt in'). Consent is for a defined purpose only and must be informed, freely given and unambiguous (see Art. 7 GDPR for the complete conditions for consent). Though consent may also be given orally, it is necessary to record the fact as you must be able to demonstrate that consent was given. Consent in writing or through electronically tracked tickboxes is advisable.

Where your lawful basis for data processing is legitimate interest, you must perform a balancing test to weigh your interests against the interests of the data subject.

Processing special categories of data is generally prohibited, unless prescribed circumstances justify such processing (see Art. 9 GDPR).

You are under an obligation to keep a record of processing activities (Art. 30 GDPR).[4]

Your systems must be designed in such a way that you will notice data breaches and you must be able to react within the time frame and in the manner prescribed by Art. 32 seqq. GDPR.

Non-compliance with the GDPR may result in significant administrative fines.

What This Means to You and Your Organization

Apart from the goal of harmonizing national law, the GDPR is the EU's effort to bring data privacy regulation up to speed in the age of Big Data. It is important to understand the extremely large scale and high relevance of data processing behind everyday operations such as using an internet search engine, online navigation or posting content on your favourite platform, etc. Keep in mind that global players perform millions of data processing operations per day and this by itself, even in the absence of breaches, can seriously impact individuals' data privacy rights. In contrast, the data

4 Comprehensive information on documentation requirements and sample records can be found here, among other places: http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ and here: https://www.bitkom.org/Bitkom/Publikationen/The-Processing-Records-Records-of-Processing-Activities-according-to-Art-30-General-Data-Protection-Regulation-GDPR.html

will likely be much smaller in scale and degree of automation. Yet, GDPR is an abstract regulation, equally applying to big and small players in the field.

It is important to realize that even as a small or mid-size NGO, you are not exempt from the principal obligations set forth by the GDPR. However, while you must abide by the established data protection principles, what is asked of you is to find and document adequate solutions under the specific circumstances in which you operate. Depending on the size of your organization, the data subjects you deal with (for example, members or employees of your organization, donors or unrelated third parties, customers and suppliers), the categories of data you process, the type, scale and impact of your processing activities vis-à-vis the data subjects' rights, this will imply different steps.

In order to reach institutional readiness, by determining and implementing the appropriate steps, an organization is likely to pass through a number of phases. And even though the time and effort needed will vary according to the nature and size of your organization and the type and scale of your data processing operations, the phases are similar for each and every one.

5 Phases to Reach and Maintain Institutional Readiness

Phase 1: Awareness and information

Understand how your organization is concerned. GDPR compliance must be made a priority of the leadership. Review internal policies and structures. Inform management and employees of steps to take and gather information on how to move forward.

Phase 2: Analysis and risk assessment

Analyze existing compliance levels and understand whether and, if so, what gap will need to be bridged to reach GDPR compliance. Start by meeting with relevant team members and compiling a list of all categories of personal data you currently hold, where it is stored (shared database systems, contact books, spreadsheets, or paper files, etc.) and how and by whom it is accessed.

Phase 3: Set the course

Develop and prioritize technical and administrative steps to be taken according to your needs, assign responsibilities.

Phase 4: Implementation

Carry out the necessary steps according to set priorities. Bring in compliance technical systems, privacy notices and internal procedures, train management and employees, complete documentation where necessary (for example, ensure you have consent if that's the lawful basis for data processing).

All of the above should be completed by 25 May 2018. But don't give up if you are not done yet! Use your best efforts to achieve the top priorities and improve as you go.

Phase 5: Monitoring and maintenance

You must be able to react swiftly to any data breach at any time. So keep alert and monitor your systems on a regular basis. Moreover, technology, law and operations will change over time. It is therefore important to maintain your systems and policies in good shape, keep learning and improving as you go. You should also continuously train your personnel and update instructions you issue to data processors down the line when necessary. This is an ongoing process and it is advisable to reasonably document maintenance activities in order to be able to demonstrate your best efforts when asked to do so.

Recommended starting points for further research:

http://data.europa.eu/eli/reg/2016/679/oj - the law (in your own language) contains a number of recitals, many of which help to understand the intention and scope of GDPR.
https://ec.europa.eu/info/law/law-topic/data-protection_en
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
https://www.institute-of-fundraising.org.uk/guidance/research/get-ready-for-gdpr/
https://www.datenschutz-bayern.de/datenschutzreform2018/ (in German)
https://protectmydata.eu/briefguide/key-issues/

7 Essential Steps to be Taken Now

For those who have already reached the end of Phase 3 as described above, this list may serve as a checklist to review the measures already taken. Technology is always evolving and so is the law. Thus, constant monitoring and adaptation (Phase 5) is essential.

For anyone else, you may find it encouraging that even as the two-year grace period comes to an end, you can achieve a reasonable level of compliance in a relatively short time, depending on the scope and scale of personal data your organization is regularly processing.

1. Increase awareness throughout your organization! Read and understand the key provisions of the GDPR.

2. Understand whether or not you need to formally appoint a Data Protection Officer (DPO, Art. 37 seqq. GDPR). While the responsibility rests with you, this support function can be delegated to a professional service provider, if necessary. Even if the law does not require you to appoint a DPO, it may be helpful to concentrate relevant knowledge in your organization.

3. Identify the categories of data and personal data relating to EU-persons within your organization. Consider the HR and public relations department and other functions that frequently deal with personal data and understand the processes.

4. Design and maintain appropriate records of data processing activities (Article 30 GDPR).

5. Identify and assess third party processing activities, ensure your contractors (processors) are GDPR compliant, and, if necessary, adapt documentation and contracts (Article 28 seq. GDPR).

6. Review the lawful basis for your ongoing processing activities and determine whether action needs to be taken, for example, whether you need to solicit consent from data subjects or perform a legitimate interest test (Article 6 GDPR).

7. Continue to monitor your regular procedures to be GDPR-compliant and train your team. This includes procedures on how to handle any privacy breach, if necessary, and how to deal with data subjects' requests.

ADF INTERNATIONAL

OFFICES

VIENNA
BRUSSELS
GENEVA
STRASBOURG
LONDON
NEW YORK
WASHINGTON DC
MEXICO CITY

ADF International is a faith-based legal advocacy organization that protects fundamental freedoms and promotes the inherent dignity of all people.

ADFinternational.org

facebook.com/ADFinternational

@ADFIntl