Schneider Law Firm

The General Data Protection Regulation (GDPR) – First Aid Action Plan for SMEs

Why the need for the GDPR?

- New developments in information technology and the way we communicate and share information
- Ensure good information handling practice
- Provide accountability of those processing personal data
- Improve individuals' data protection rights

First Aid Action Plan for SMEs

1. Does **the GDPR apply** to our occupation? (Are we working with personal data?)
2. Is our **processing** of personal data lawful **according to Articles 6 and 5** GDPR?
3. Do we have **adequate privacy notices** according to Articles 13 and 14 GDPR?
4. Prepare **records of processing activities** according to Article 30 GDPR
5. Are we engaging another processor-companies to process personal data on our behalf? If so, is there a **contract compliant with the requirements of Article 28** GDPR?
6. Do we need to designate a **data protection officer** according to Article 37 GDPR?
7. Are we prepared to comply with **data subject rights** according to Articles 15-22 GDPR?
8. What do we have to do in case of a **personal data breach**? (Articles 33, 34 GDPR)

The Structure of this Presentation

- We will discuss the above stated „First Aid Action Plan“

The Purpose of this Presentation

- To provide you with a solid foundation for the implementation of the GDPR

STEP 0: Download the text of the GDPR

The official text of the GDPR can be downloaded in numerous languages at:

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679

The GDPR consists of Recitals (1-173) and Articles (1-99).

It is highly recommended that you read the text of the Articles that are discussed in this presentation.

STEP 1: Does the GDPR apply to our occupation? (Are we working with personal data?)

- **“Personal data”:** VERY broad and even includes "online identifiers" (e.g. IP address), location data, tax number.

- **“Processing”:** also VERY broad ⇨ ANY action involving personal data (e.g. collecting, saving, changing, erasing). Includes restricting data i.e. marking data to limit its future use.

- **Ask youself:**

  - Am I offering goods or services within the EU?

  - Do I have employees?

- If you answered **one** of the questions with “**yes**”, you are processing data and the GDPR applies to you or your business, i.e. you have to observe its provisions.
- **Exception**: no processing of personal data (i.e. GDPR does not apply), if by a natural person in the course of a purely personal or household activity.

STEP 2: Is my processing of personal data lawful according to Article 6 and Article 5 GDPR?

The processing of personal data has to be „lawful“ according to the criteria of Article 6 (1) GDPR and according to the principles of Article 5 (1) GDPR.

- The most important criteria of Article 6 (1) GDPR:

- Consent to the processing by the data subject: high requirements for constent, read Article 4 No 11
- Processing is necessary for the performance of a contract (e.g. name, address)
- Processing is necessary for the purposes of the legitimate interests pursued by the controller

STEP 2 continued: Is my processing of personal data "lawful" according to Article 6 and Article 5 GDPR?

The most important principles of Article 5 (1) GDPR:

- Purpose limitation (example: If I sold a customer a car, I cannot use its data to market real estate to it)
- Accuracy (the data has to be current and correct)
- Storage limitation (the data that are not required anymore, have to be erased, i.e. data can be saved only for a particular purpose and for a particular time)
- Accountability (you have to be able to prove to the Supervisory Authority how you observe the Articles 6 and 5 GDPR)

STEP 3: Do we have adequate privacy notices according to Articles 13 (and 14) GDPR?

1	Identity and contact details of data controller and contact details of DPO (if applicable)	7	Whether any automated decision making and consequences of that processing
2	Purposes and basis for processing (if using legitimate interests state what those interests are)	8	Data retention period (or how that will be determined)
3	Right to withdraw consent (if relying on consent)	9	Recipients/categories of recipient of data (e.g. if data will be shared)
4	Categories of data processed	10	Details of any transfers outside Europe including how data will be protected and how individuals can obtain copies of safeguards e.g. transfer agreements
5	Source of data including any public sources	11	Individuals' rights including right to object to marketing, right to be forgotten, port data, make a subject access request
6	Whether providing data is contractual or statutory requirement and any consequences of not providing it	12	Right to complain to supervisory authority e.g. ICO

STEP 4: Prepare records of processing activities according to Article 30 GDPR

- The exception of Article 30 para 5 almost never applies, since almost all businesses conduct payroll accounting or almost all associations conduct management of member data

- The record is for small companies not difficult to compile. The minimum contents as per Article 30 (1) GDPR are:

- the name and contact details of the controller (e.g. Maria Müller, Human Resources, Address, Tel. & Mail)
- the purposes of the processing (e.g. payroll accounting of employees for the purposes of employment)
- a description of the categories of data subjects and of the categories of personal data (names, addresses, etc of employees)
- the categories of recipients to whom the personal data have been or will be disclosed (e.g. tax accountants, social security authorities, etc)
- where possible, the envisaged time limits for erasure (e.g. 10 years after termination of employment)

STEP 5: Are we engaging another processor-companies to process personal data on our behalf?

Data processing by 3rd parties on your behalf:

- This is the case when you decide the purposes and means of processing, i.e. the 3rd party processes the data according to your instructions.

  Example: payroll accounting done by an external accountancy firm

- This is not the case, when you are just getting professional advice. Example: financial advice or tax advice.

STEP 5 continued: If yes, do we have a contract according to the requirements of Article 28 GDPR?

You and the 3rd party processor must conclude a contract that complies with the requirements of Article 28 GDPR.

This is especially important if you are the 3rd party processor yourself (e.g. you are the accountancy firm from the above example).

The content of the contract must be as specified by Article 28 (3)!

ART 28 (3):

The contract has to set out:

- the subject-matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subjects
- the obligations and rights of the controller
- Further specifications as per Article 28 (3) (a) – (h), e.g.:

ART 28 (3) continued:

- Process only on controller's written instructions (including any processing outside Europe)
- Use appropriate data security measures to same level as mandated for controllers
- Ensure staff work under obligation of confidentiality
- Assist controller with data subject rights e.g. subject access, right to erasure
- Assist controller in compliance with data security obligations
- Make relevant info available to controller and co-operate with audit
- Use sub-processor only with controller's permission & flow down processing obligations

IMPORTANT: Check your old contracts for the compliance with the requirements of Article 28 GDPR. If they do not comply, they have to be amended accordingly!

STEP 6: Do we need to designate a data protection officer (DPO) according to Article 37 GDPR?

When do you need to appoint a DPO?

The appointment of a DPO is mandatory for the following organisations:

- Organisations whose core activities involve regular, systematic and large-scale monitoring of data subjects. Examples: debt collection agencies or organisations which provide commercial information services.

- Organisations whose core activities consist of the large-scale processing of special categories of data. Examples: data concerning health, sexual orientation, race, religion, political affiliations, criminal convictions.

STEP 7: Prepare to comply with data subject rights – Article 21 – right to object

- Key aim of GDPR is to place individual at heart of data protection ⇨ data subjects' rights expanded and bolstered
- Article 21: Individuals have the right to object to processing:
  - Direct marketing and
  - Processing based on legitimate interest (or task in the public interest)
- Legitimate interests ⇨ stop unless controller can show compelling reasons why legitimate interests override individual's rights or processing is to establish/defend/exercise legal rights
- Burden of proof: controller must show why processing should continue

STEP 7 continued (data subjects' rights – Article 17 - right to erasure)

- Individual can request erasure when:
  - Data no longer needed for original purpose
  - Withdrawal of consent (if no other condition for processing)
  - Objection to use of legitimate interests and controller cannot show overriding reasons to continue
  - Data processed in breach of GDPR – potentially wide right
  - Legal obligation on controller to erase
- If data put in public domain controller must take reasonable steps to inform other controllers of erasure request ⇨ highly relevant online

STEP 7 continued (data subjects' rights – Article 15 - subject access)

- Copy of all personal data held by controller, cf. Article 15 (1) (a)-(h)
- Time limit reduced to maximum one month, with limited ability to extend by a maximum of two further months
- Data to be provided in commonly used electronic format
- Supplemental information: e.g. details of disclosure to recipients outside Europe, retention period, right to rectification/erasure/ restriction of processing and right to complain to supervisory authority
- Controller can refuse requests that are manifestly unfounded or excessive (or charge a fee)

STEP 8: What do we have to do in case of a personal data breach? (Articles 33, 34 GDPR)

- Under GDPR obligation on controllers to inform supervisory authority and (potentially) individuals in the event of **some** data breaches
- "Data breach" is widely defined – includes unauthorised access and alteration, not only data loss
- Reportable incident is a "*breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data* "
- Exemption from notification: if breach unlikely to cause a risk to individuals – but must still document it

STEP 8 continued: What do we have to do in case of a personal data breach? (Articles 33, 34 GDPR)

- Must report to supervisory authority promptly and where feasible within 72 hours of becoming aware of incident
- Controller must also report to individuals unless:
  - Breach unlikely to affect their rights and freedoms (e.g. financial loss, identity theft, damage to reputation, see Recital (85) for further details)
  - Controller had taken measures to protect the data e.g. encryption
  - Notification would involve disproportionate effort – if so, use public communication e.g. notice in newspaper, website announcement
- Processor must inform controller swiftly once aware of incident

Schneider Law Firm

Download this presentation and other free material from our website:

http://www.law-schneider.com/checklists.html