SZECSKAY ATTORNEYS AT LAW
WWW.SZECSKAY.COM

WE CARE. WE DARE. WE EXCEL.

QUICK GUIDE

Tips to prepare for compliance with the EU's General Data Protection Regulation

The contents of this handbook are intended to provide only a general overview of the subject matter. Specialist advice should be sought for specific matters. Queries relating to this guide should be addressed to the authors at:

ZOLTAN.KOVACS@SZECSKAY.COM, LASZLO.POK@SZECSKAY.COM

Introduction

Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**Regulation**") will replace Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**Directive**"). The Regulation will be enforced after 25 May 2018, thus, entities are required to prepare for compliance by then.

What does this mean and what main novelties will the Regulation bring about?

- **Change in concept**: The Regulation is directly applicable and effective in all member states of the EU. The purpose is to have standardized data protection laws throughout the Union. However, the Regulation allows members states to specify or supplement certain rules. Result: There will be no fully unified data protection regime in the EU but data protection laws of member states will be much closer to each other than under the Directive. (There may be more deviations as regards procedural rules.)

- **Main novelties**: extraterritorial scope, data portability, right to be forgotten, privacy by design, privacy by default, high amount of fine, pseudonymisation, profiling, data protection impact assessment, data breach notification, cooperation and consistency mechanism, etc. For details, see below under the relevant chapter.

What should data controllers do to comply with the Regulation?

- Data controllers should get familiar with the provisions of the Regulation as soon as possible.

- It is worth checking the available guidelines of the DPAs and the European Data Protection Board regarding the application of the Regulation.

- The data processing activities must be reviewed in the light of the provisions of the Regulation. Necessary changes must be implemented before May 25, 2018.

- If a new data processing activity is planned, its compliance with the Regulation should be ensured, even before May 25, 2018, to save time and costs.

Scope

The Regulation is wider in territorial scope than the Directive as it has an extraterritorial effect.

Basically, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

However, the Regulation also applies to

the processing of personal data of individuals who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
a) offering goods or services to such individuals in the Union (no matter if the goods or services are free) **[language and currency may be indicative of the intention to offer goods or services to individuals in the EU]**,
b) the monitoring of individuals displayed within the Union **[e.g. tracking persons on the Internet]**.

Conclusion:

Data controllers and processors are advised to check if their activities are covered by the Regulation.

Privacy by design / Privacy by default

New mindset required:

When establishing operations, data controllers are required to implement appropriate technical, organizational and security measures designed to implement data protection principles in an effective manner ("privacy by design"). **[Such principles are: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity.]**

Data controllers must implement appropriate technical and organizational measures which ensure that only personal data necessary for the specific purpose are processed ("privacy by default").

Conclusion:

The Regulation requires data controllers to design their operations from the very beginning in a way that they also take into account the data protection rules.

Data controllers are advised to check if their activities take into account such rules.

Lawfulness of processing

Processing of personal data is lawful only if and to the extent that at least one of the following applies:

(i) the data subject has given consent to the processing;
(ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(iii) processing is necessary for compliance with a legal obligation to which the controller is subject;
(iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(v) processing is necessary for the performance of a task carried out in the public interest;
(vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (assessing different interests).

Conditions of consent are also regulated.

Special rules apply to the lawfulness of processing special categories of personal data (e.g. medical data).

Children enjoy a specific protection with regard to the processing of their personal data.

Conclusion:

The legal basis of data processing must be granted by data controllers.

Data controllers must be prepared to demonstrate that the data subject has consented to the processing of his or her personal data.

Records of processing activities

This obligation applies to both data controllers and data processors.

Data controllers must maintain a record of processing activities, which has to contain

- the name and contact details of the controller, and, where applicable, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards;
- where possible, the envisaged time limits for the deletion of the different categories of data;
- where possible, a general description of the technical and organizational security measures taken.

Data processors must maintain a record of processing activities, which has to contain

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures taken.

Exemption from keeping records:

The obligation does not apply to an entity employing fewer than 250 persons **unless**

- the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects,
- the processing is not occasional, or
- the processing includes special categories of data (sensitive data) or personal data relating to criminal convictions and offences.

Conclusion:

Data controllers and data processors must examine if they are required to prepare records of processing activities and, if they are, they have to maintain such records and have to be ready to provide such records to the supervisory authority upon request.

Data protection impact assessment

This obligation applies to data controllers.

"Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

In particular, an impact assessment must be prepared in the case of:

(i) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. automated credit assessment, automated performance evaluation);
(ii) processing on a large scale of special categories of data (e.g. health data), or of personal data relating to criminal convictions and offences; or
(iii) a systematic monitoring of a publicly accessible area on a large scale (e.g. operation of surveillance camera in a store).

The assessment must contain at least:
- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The controller has to consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risks and the controller sees no way to mitigate such risks.

Conclusion:

Data controllers are advised to check their activities and clarify if they need to prepare a data protection impact assessment.

Data breach notification

Both data controllers and data processors have certain obligations.

Data controller is required to **notify the DPA** of the data breach without delay but, at the latest, within 72 hours from the occurrence of the incident, if the breach is likely to result in a risk to the rights and freedoms of natural persons. (If no notification is made within 72 hours, reasons for the delay must also be submitted.)

The notification must at least

(i) describe the nature of the data breach, including the categories and number of persons concerned and the data;

(ii) contain the name and contact details of the data protection officer or contact person;

(iii) describe the likely consequences of the incident;

(iv) describe the measures taken or proposed to be taken to address the data breach and mitigate possible adverse effects.

Data processor must inform the **data controller** of such a breach without delay.

Data controller must **keep a registry** of all data protection breaches including the facts and effects of the breach and the measures taken to mitigate the consequences.

Data controller is **required to inform the persons** affected of the breach if the breach is likely to result in a high risk to the rights and freedoms of the persons concerned. As to content, see notification to the DPA.

No notification to the persons concerned is necessary if

(i) the controller has implemented appropriate technical and organizational protection measures and those measures were applied (e.g. encryption which rendered the data unintelligible to any person not authorized to access it);

(ii) the controller has implemented appropriate measures which ensure that the high risk to the rights and freedoms of persons is no longer likely to materialize;

(iii) it would involve disproportionate effort.

Conclusion:

Data controllers must keep a registry on data breaches and be ready to inform the DPA and the persons concerned of such breaches.

Data processors are advised to be ready to inform the data controllers of any data breach.

Data protection officer (DPO)

This obligation applies to both data controllers and data processors.

Data controllers and data processors must appoint a DPO if e.g.
i) 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; or
ii) the core activities of the controller or the processor consist of processing a large scale of special categories of data (sensitive data, personal data relating to criminal convictions and offences).

Tasks of the DPO:
(i) informing the controller or the processor and the employees in connection with the Regulation;
(ii) monitoring compliance with the Regulation;
(iii) advising in connection with the data protection impact assessment;
(iv) cooperating with the DPA;
(v) acting as a contact person for the DPA.

Conclusion:

Data controllers and processors are advised to examine if they are required to appoint a DPO and, if they are, a DPO must be appointed prior to 25 May 2018.

Designation of representative

This obligation applies to both data controllers and data processors.

In connection with the extraterritorial effect of the Regulation, **data controllers and data processors without an establishment in the EU** are required to designate in writing a representative in the EU if they

(i) offer goods or services to individuals in the Union (no matter if the goods or services are free), or

(ii) monitor the behaviour of individuals within the EU as far as they take place within the Union.

Exemption:

The obligation to designate a representative does not apply to

(i) processing which is **occasional** and **does not include**, on a large scale, the processing of special categories of data or the processing of personal data relating to criminal convictions and offences, and which **is unlikely to result in a risk** to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(ii) a public authority or body.

Conclusion:

Data controllers and processors are advised to examine if they are required to designate a representative and, if they are, a representative must be designated prior to 25 May 2018.

Transfer of personal data

This applies to both data controllers and data processors.

Legal basis for transfer:

- **Adequacy decision**
- **Appropriate safeguards** (including also the application of binding corporate rules (BCR))
- **Specific situations** (e.g. informed consent; contract; assertion of claims; the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.)

Conclusion:

The legal basis for the transfer of personal data must be ensured by the data controller.

Administrative fine

The DPA will have the power to impose a fine on non-compliant entities.

The maximum amount of the fine may be **EUR 20 million and 4% of the total worldwide turnover** of the relevant entity for the preceding financial year, whichever is higher.

The amount of the fine depends on a number of factors, such as, for example,

- the nature, gravity and duration of the infringement, taking into account the number of persons affected and the level of damage caused;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented;
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- where certain authority measures have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- adherence to approved codes of conduct or approved certification mechanisms; and
- any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, due to the infringement.

Conclusion:

Compliance with the Regulation must be handled as a high priority.

Cooperation and consistency mechanism

Cooperation mechanism:

National DPAs will cooperate from 25 May 2018.

The **lead supervisory authority** (LSA) will be the DPA of the member state where the data controller / data processor has its main establishment.

Forms of cooperation:
(i) cooperation between LSA and other DPAs;
(ii) mutual assistance;
(iii) joint operations.

Consistency mechanism:

In order to contribute to the consistent application of the Regulation throughout the Union, the DPAs cooperate with each other (through the European Data Protection Board) and, where relevant, with the Commission.

The European Data Protection Board has an important role in ensuring the consistent application of the Regulation. (The Board will take over the role of the Working Party under Article 29.)

The consistency mechanism will be two-fold:
(i) the Board issues opinions;
(ii) the Board resolves disputes.

The Board issues an opinion where a competent DPA intends to adopt certain measures (e.g. a list of activities for which a data protection assessment must be prepared, a code of conduct, BCR, standard data protection clauses.)

In order to ensure the correct and consistent application of the Regulation in individual cases, the Board adopts a **binding decision** in the following cases:
(i) where, during the cooperation mechanism, a DPA concerned has raised a relevant and reasoned objection to a draft decision of the LSA or the LSA has rejected such an objection as being not relevant or reasoned;
(ii) where there are conflicting views on which of the DPAs concerned is competent for the main establishment of the data controller/processor;
(iii) where a competent DPA fails to request the opinion of the Board or does not follow the opinion of the Board. In that case, any DPA concerned or the Commission may communicate the matter to the Board.

Rights of persons concerned

- **Right of access to personal data** and information about the purposes, category of personal data, recipients, duration of processing, rectification / erasure / objection, right to file a complaint with the DPA, source of data and on profiling;
- **Right to rectification**;
- **Right to erasure, „right to be forgotten"** (Google decision);
- **Right to restriction of data processing** (if e.g. the processing is unlawful and the data subject does not request deletion but rather restriction, or if the controller no longer needs the data for a specific purpose but they are required by the data subject for the exercise of legal claims;
- **Right to data portability** (The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where (a) the processing is based on consent or on a contract and (b) the processing is carried out by automated means);
- **Right to object** (e.g. in the case of direct marketing or profiling);
- **Profiling**: The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This rule is not applicable if the decision

(a) is necessary for the entering into of, or the performance of, a contract between the data subject and the controller;
(b) is authorized by Union or member state law to which the controller is subject and which also lays down suitable measures for safeguarding the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.

Conclusion:

Data controllers must be prepared to be able to fulfill the lawful requests of the persons concerned (e.g. right to be forgotten, data portability).

Things to do

- Data controllers and processors are advised to check if their activities are covered by the Regulation.

- Data controllers are advised to check if their activities properly take into account data protection principles.

- Data controllers are advised to review the legal basis of their data processing activities.

- Data controllers must be prepared to demonstrate that the data subject has consented to the processing of his or her personal data.

- Data controllers and data processors must examine if they are required to prepare records of processing activities and, if they are, they have to maintain such records and have to be ready to provide such records to the DPA upon request.

- Data controllers are advised to check their activities and clarify if they need to prepare a data protection impact assessment.

- Data controllers are advised to keep a registry of data breaches and be ready to inform the DPA and the persons concerned of such breaches.

- Data processors are advised to be ready to inform the data controllers of any data breach.

- Data controllers and processors are advised to examine if they are required to appoint a DPO and, if they are, a DPO must be appointed prior to 25 May 2018.

- Data controllers and processors are advised to examine if they are required to designate a representative and, if they are, a representative must be designated prior to 25 May 2018.

- Monitoring and following the guidelines, recommendations and best practices of the Board is important as they will play an essential role in interpreting the provisions of the Regulation.

- Data controllers must be prepared to fulfill the lawful requests of the persons concerned (e.g. the right to be forgotten, data portability).

- It is advisable to apply pseudonymisation as much as possible.

The contents of this handbook are intended to provide only a general overview of the subject matter. Specialist advice should be sought for specific matters. Queries relating to this guide should be addressed to the authors at:

ZOLTAN.KOVACS@SZECSKAY.COM, LASZLO.POK@SZECSKAY.COM