1 Year ahead of the GDPR Application – a Checklist

As of 25 May 2018 the Regulation (EU) 2016/679 (General Data Protection Regulation) ("**GDPR**") will apply. The GDPR will establish new, EU-wide uniform data protection rules. In its statement of 24 May 2017, the European Commission emphasizes the benefits for EU citizens ("gaining control of one's personal data") and businesses ("one continent, one law") (EU Commission Statement dated 24 May 2017). For businesses, however, the new GDPR rules entail considerable organizational and management efforts. The clock is ticking – from now on one year is left for businesses to adopt their data management processes to the GDPR requirements. Companies not complying with the GDPR requirements risk administrative fines up to 20 million EUR or 4% of the total worldwide annual turnover.

In the following, we summarize the benefits for businesses and provide a checklist of key changes which should be duly considered when companies adjust their "data housekeeping" to the GDPR standards.

I. Benefits for businesses

- One continent, one law": The GDPR replaces the current "inconsistent patchwork" of 28 different national data protection laws. Companies will deal in future only with a single law.
- "One-stop-shop": Companies will only have to deal with one single supervisory authority, not 28, making the administrative procedures simpler and cheaper.
- Territorial level playing field: The GDPR rules will create a level playing field because the GDPR applies regardless of whether the processing of personal data takes place in the EU or not: Companies processing personal data which are based outside of the EU have to comply with the same rules as EU companies when they offer goods or services on the EU market to individuals ("**Data Subject(s)**") or are monitoring the behaviour of Data Subjects within the EU.

II. Key Changes Checklist

The following checklist lists some key changes to the legal framework by the GDPR rules to be

considered when companies are adapting their data protection processes and practices to the GDPR.

- **Apply the stricter data processing principles**

Processing of personal data must conform to the data processing principles (Article 5), and must, in particular, (be):

  - Made in a lawful, fair and transparent manner (➔ *Note*: information duties towards Data Subjects; more stringent consent requirement, etc.);
  - Collected only for the specified, explicit and legitimate purposes and no further processing purposes (➔ *Note*: consider when changing the processing purposes);
  - Stored only for the period allowed by law, no longer (➔ *Note*: Implementation of time limits for storage/ periodic review/ anonymising data);
  - Ensure that personal data which are inaccurate are rectified or deleted (➔ *Note*: Compliance with the Data Subject's rights);
  - Ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damages (➔ *Note*: Implementation of appropriate technical and organizational measures ("**TOM(s)**")).

- **Regard the Data Subject's rights**
  - *Information on personal data (Article 13-14):*

    The Data Subject must be informed of the processing operation and its purposes and all information necessary to ensure fair and transparent processing (e.g. the contact details of the controller, and, where applicable, of the controller's representative, and, the data protection officer).

  - *Data Subject's rights (Article 15-22):*

    Data Subjects must be given access to the personal data collected on them; Data Subjects can demand *inter alia*: rectification of inaccurate personal data, erasure of personal data ('right to be forgotten'), restriction of processing, transmission of their data to another data controller ('data portability right').

  ➔ *Note:* compensation claims by individuals are possible.

- **Comply with the organizational duties for data controllers**

Data controllers will have to implement viable accountability processes with regard to:

  - *Data breaches (Article 33, 34):*

    Controller must notify data breaches (i) not later than 72 hours after having become aware of it to supervisory authorities and (ii), where the "data breach is likely to result in a high risk to the rights and freedoms of natural persons", without undue delay to affected Data Subjects.

  - *Record of processing activities (Article 30):*

    In order to demonstrate compliance with this Regulation, the controller (or processor, where applicable) must maintain records of processing activities and make those records, on request, available to the supervisory authorities *(*➔ *Note*: Record-keeping does not apply to companies with less than 250 employees (but there are exceptions, e.g. where risks for the Data Subjects' rights are likely)).

- *Data protection impact assessment ("**PIA**") (Article 35):*

  The controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, where data processing is likely to result in a high risk to the rights and freedoms of "natural persons".

- *Data protection officer ("**DPO**")(Article 37):*

  Where the core activities of processing consist of processing operations

  (i) that require regular and systematic monitoring of the Data Subjects on a large scale, or,

  (ii) on a large scale of special categories of personal data and data relating to criminal convictions and offences,

  the controller (and in case (ii) also processor) must be assisted by a DPO, who has expert knowledge of data protection law and practices to monitor internal compliance with the GDPR.

- *Data protection by design and by default (Article 25)*:

  The GDPR obliges the controller to implement internal policies and TOMs that meet the principles of data protection by design and data protection by default (e.g. through minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the Data Subject to monitor the data processing, enabling the controller to create and improve security features (Recital 78)).

  Producers of new products or services have to take into account, when developing and designing, the right to data protection, and, to make sure that controllers and processors are able to fulfil their data protection obligations.

- **Adapt data processing agreement(s) ("DPA(s)")**

  Seen from the German law perspective much remains as known. However, the new duties and responsibilities under the GDPR must be reflected in new DPA(s) e.g.:

  - The GDPR obliges the processor to (i) assist the controller in complying with notification/ information, security and PIA duties (Art. 32-26) and (ii) make available to the controller all information necessary to demonstrate compliance with the obligations (➔ *Note*: Establish processes for the communication and documentation and implement on controller and processor side).

  - Controller and processor are jointly liable (*Gesamtschuldner*) towards a person who suffered a material or non-material damage as a result of an infringement of the GDPR (Article 82(4) GDPR)) (➔ *Note*: Consider commercially and/or contractually).

- **Pay due consideration to data transfer rules**

  The GDPR does not change the current rules for cross-border transfers of personal data substantially; the principles as under the Data Protection Directive stay the same. However, observance of data transfer rules is key for businesses: the infringement of transfer provisions can be sanctioned by fines up to 20 million EUR, or, in the case of undertakings, up to 4% of the annual worldwide turnover.

- **Adjust processes by keeping in mind the fines risks**

  The amount of fines for non-compliance with the GDPR depends on the circumstances of each individual case. The GDPR sets two ceilings for fines: (i) fines setting an amount up to 10 million EUR or, in case of an undertaking, up to 2% of worldwide annual turnover (e.g. if a controllers does to conduct required PIA(s)), and, (ii) fines reaching up to 20 million EUR, or 4% of worldwide annual turnover (e.g. for an infringement of the Data Subjects' rights under the GDPR) (➔ Note: Consider these risks when classifying, drawing up and reviewing processes).

III. 'To Dos' for businesses

Companies should check if all requirements of the GDPR have already been considered in the reorganization of the company's data protection system. The implementation of structured processes for data processing and risk management are highly recommended in view of the high administrative fines for the failures to comply with the GDP. The 'To Do' for businesses in the remaining 12 months is reviewing, refining and testing the data managements processes established.

Written by Hendrike Wulfert-Markert

For further information please contact

Dr. Lars Lensdorf

Tel: +49 (69) 768063-30
Mobile: +49 (160) 90704902
E-Mail: l.lensdorf@heylaw.de

Dr. Moritz Hüsch, LL.M.

Tel: +49 (69) 768063-453
Mobile: +49 (151) 12577724
E-Mail: m.huesch@heylaw.de