CED Guidance on the Implementation of the General Data Protection Regulation
Focus on the Data Protection Officers
February 2018

Context

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the EU.
- The Regulation – in Chapter IV, Section 4, Articles 37-39 - specifies requirements about the designation, position and tasks of Data Protection Officers (DPOs).

Why is this important for dentists?

- National administrations now need to implement the provisions of the GDPR and could require dental practices to appoint a DPO.
- While the guidance of the Article 29 Data Protection Working Party – the advisory body on processing of personal data – states that individual doctors (the same would apply to dentists) do not need a DPO, Member States are not bound by this guidance and it is unclear when exactly a DPO needs to be appointed.
- Depending on the national implementation, this could lead to an increase in administrative and financial burden for individual dentists.

Timelines

- The Regulation was published in April 2016.
- It will apply from 25 May 2018.

Required Action

- Get in touch with your administration to identify at which state of the implementation they are and what their thinking is on DPOs.
- Identify a workable solution for dentists (i.e. define the threshold for requiring a DPO by using the below guidance) in your national context and provide it to the authorities.

Recommendations

- In general, the CED stresses that data protection should be taken very seriously. Patient data needs to be safeguarded with utmost caution.

- Data Protection Officer
    - The GDPR states that a DPO should be appointed where the core activities of the controller or the processor (in our case the dental practice or the dentist) consist of processing operations which require regular and systematic monitoring of data subjects on a large scale.
    - Therefore there are two criteria to be taken into account when discussing whether a DPO is needed:
        - How many people does the dental practice include whose core activity it is to process data?
        - Is data processed on a large scale?
    - **Criteria 1: Core Activity**
        - In our view, it is not a core activity of the dentist to process data, but a requirement to treat patients (the actual core activity). At the same time, dentists may have staff whose core activity it is to process patient data. If there is no significant number of staff whose core activity is data processing, a DPO should not be required.
    - **Criteria 2: Large Scale**
        - The Article 29 WP gives further guidance on how to define large scale:
            - The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
            - The volume of data and/or the range of different data items being processed
            - The duration, or permanence, of the data processing activity
            - The geographical extent of the processing activity
        - At least two of these criteria should show that the office in question processes extraordinary amounts of data in order to require a DPO. The average dental practice should therefore not be considered as processing data on a large scale.
- **Data Protection Impact Assessments**
    - We believe that the same criteria should apply to evaluate whether to fulfil the requirements introduced by the GDPR for so-called Data Protection Impact Assessments (DPIAs) – Chapter IV, Section 3, Articles 35-36 – to be done where the use of new technologies for data processing are likely to result in high risks to the rights and freedom's of persons.

If you need support from the CED Office, do not hesitate to contact us.

****

Background – Main changes under the GPDR and how they differ from the previous Directive

(Source: https://www.eugdpr.org/the-regulation.html)

Penalties

The Regulation sets two ceilings for fines if the rules are not respected: 1) fines up to a maximum of €10 million or, in case of an undertaking, up to 2% of worldwide annualturnover. This first category of fine would be applied for instance if a controllers does not conduct impact assessments, as required by the Regulation; 2) a maximum of €20 million or 4% of worldwide annual turnover. An example would be an infringement of the data subjects' rights under the Regulation. Fines are adjusted according to the circumstances of each individual case.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic fromat. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it’s core, privacy by design calls for the

inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the

breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.