OXFORD
ORTHODONTIC CENTRE

General Data Protection Regulation (GDPR) Policy

Introduction

The GDPR has replaced the Data Protection Act 1998 (DPA) and radically overhauls many of the existing data protection rules.

Accountability & Data Governance

One of the main features of the GDPR is that compliance alone is not enough; data controllers will also have to demonstrate their compliance and prove that they are taking data protection seriously by implementing a range of accountability measures. These measures include Privacy Impact Assessments, data protection audits, policy reviews, activity records and in some cases, the mandatory appointment of a DPO.

Here is an overview of some of the accountability measures you will need to understand:

Privacy Impact Assessments

Privacy Impact Assessments PIAs will need to be carried out when we are planning a new initiative which involves "high risk" data processing activities i.e. where there is a high risk that an individual's right to privacy may be infringed such as monitoring individuals, systematic evaluations or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies such as biometrics.

The idea behind a PIA is to identify and minimise non-compliance risks.

Pseudonymisation

This new term refers to the technique of processing personal data in such a way that it can no longer be attributed to a data subject without cross referencing it with other further information. The further information must be kept separate and subject to technical and organizational security measures to ensure that the data subject cannot be identified.

Pseudonymised information is still a form of personal data but the GDPR promotes its usage in certain circumstances in order to enhance privacy and contribute to overall compliance.

E.g. GDPR may expect pseudonymisation to be considered when personal data is processed in a way which is "incompatible" with the purposes for which it was originally obtained. Alternatively, the technique could be appropriate for practices wishing to use employee data for historical or statistical purposes.

Data Protection Audits

We need to review and document the personal data we hold, identify the source and who it is shared with. This exercise is commonly called a data protection audit. We can demonstrate how we comply with the data protection principles in practice.

Another critical benefit of a data protection audit is that it maps flows of personal data into and out of the practice and can be used to measure the degree to which the practice complies with the law and identify "red flags" which require urgent attention.

Data Protection Policy Reviews

All practice policies have been reviewed, particularly those relating to data protection. Data protection policies are used to explain an individual's legal rights and how those rights can be exercised. Because the GDPR amends those rights, our policies have been amended.

Any policies also intended to be read by children will now be explained in clear non – technical language and in a way, that can be readily understood by the intended audience.

Appointment of a Data Protection Officer (DPO)

Due to the significant new burdens imposed on data controllers by GDPR, all practices now formally must appoint a DPO.

The DPO for the practice is Sadaf Khan who has received training in this area.

The DPO has specific knowledge of the sector. The employer must help the DPO maintain this knowledge e.g. by making provision for specific training.

The DPO's tasks as a minimum include: advising colleagues and monitoring the practice's compliance including via staff training and awareness raising; advising on PIAs; being the point of contact for supervisory authorities; developing policies and procedures; watching out for publication of relevant guidance and Codes of Practice; monitoring the documentation, notification and communication of data breaches.

A DPO can be an employee or a hired contractor

The DPO can work "independently of instruction" and not dismissed or penalised simply for doing their job.

The DPO's contact details must be published and registered with the supervisory authority. They will be the point of contact for compliance matters.

Staff Data Protection Training

Practices will continue to be subject to an obligation to take organisational steps to keep personal data secure and the deployment of staff data protection training will continue to be expected. New starters will receive data protection training before they have access to personal data and existing staff will receive regular and refresher training.

Practice that breach the GDPR will be criticised if they have failed to ensure that all staff that handle personal data have received data protection training. This is because, staff training is a simple organisational measure that an organisation can take to reduce the likelihood of data losses.

All staff that have access to personal data will receive mandatory basic data protection training and key staff that need to know more will get enhanced training. We will keep records of who has received training and when and ensure that those staff who did not attend (for whatever reason), get trained as well.

Communicating

Data Protection/Privacy Information

GDPR requires us to provide much more meaningful information to individuals about how we use their data.

Under GDPR, the list of information which must be provided to individuals will increase significantly. Some of the information has to be communicated in all cases (mandatory Privacy Notice information) whilst a second subset of information need only be provided in specific cases e.g. if the practice intends to process the personal data for further different purposes than those that existed at the time of collection. Notwithstanding the sheer volume of information that now needs to be included in our Privacy Notice, we will be expected to provide this in a concise, transparent, intelligible and easily accessible way. Here is some of the information you will be expected to provide:

Your Identity and Contact Details

The Purpose of processing data and the legal basis for the processing of that data. (This later requirement is new and will require significant thought in some cases.)

- Who we share the personal data with
- Transfers outside EU and how data is protected
- Retention period or criteria used to set this
- Tell individuals' all their legal rights e.g. the right to withdraw their consent to their data being used for marketing or for practice fundraising

Legal Ground for Processing Personal Data

GDPR sets out conditions (or grounds) that must be met for the processing of personal data to be lawful. For example, personal data may be processed with consent or where the processing is necessary for a contract or where the processing is necessary for compliance with a legal obligation.

Under the GDPR we will need to know our legal grounds for processing personal data and in some cases, explain it to staff, for example, it is likely that our legal ground for processing staff images for identification purposes will be because the processing is necessary for the contract. In contrast, the legal ground for using staff images for marketing and on the website is likely to be consent.

We will have to explain our legal grounds for processing personal data in our Privacy Notice or when answering a Subject Access Request. This is new.

Under the GDPR, some individuals' rights are modified depending on our legal basis for processing their personal data. For example, individuals will have a stronger right to have their data deleted where we use consent as our legal basis for processing.

Consent

We have reviewed how we see and record consent for the processing personal data and consider if any changes are required under the GDPR.

Under GDPR, consent of a data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed.

Freely given: The consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place.

Specific: Separate consents must be obtained for different processing operations. It must be distinguishable from other matters and not "buried" in wider written agreements. Under GDPR there is a presumption that consents should be separable from other written agreements. (This could require attention since many standard contracts incorporate consents for a multitude of other processing activities such as marketing. Practices should therefore be prepared to separate processing activities which are based upon and require consent from those which are actually based upon contractual necessity.)

Fully informed: You should clearly explain to individuals what they are consenting to and of their right to withdraw consent.

Consent must be unambiguous and be a positive indication of agreement: It cannot be inferred from silence, inactivity or pre-ticked boxes.

Individuals Rights

The legal rights that individuals have under GDPR are very similar to those they currently enjoy under the DPA. However, there are some significant enhancements and amendments which you need to be aware of.

The main legal rights under the GDPR include:

The right of subject access (see below);

- To have inaccuracies corrected
- To have information erased (the so called "right to be forgotten")
- To prevent direct marketing (i.e. where marketing is directed to specific individuals)
- To prevent automated decision-making and profiling, and
- Data portability (This is a new enhancement to the right of subject access. In brief practices will have to provide requested information electronically and in a commonly used machine-readable format)

Right of Subject Access

The GDPR will continue to allow individuals to ask to give them a copy of their personal data together with other information about how it's being processed by the practice. (This is known as a Subject Access Request or SAR for short).

Under GDPR the rules for handling SARs will change and we have updated its procedures accordingly and plan for how it will meet the new deadlines and other new requirements.

Under GDPR, the main changes are:

- Now free in most (but not all) cases (used to be £10)
- Manifestly unfounded or excessive requests can now be charged for or refused
- Deadline reduced from 40 calendar days to "within 1 month". This deadline can be extended in certain cases.
- Additional information to be supplied e.g. data retention periods and the right to have inaccurate data corrected.
- If you want to refuse a SAR, you will need to have policies and procedures in place to demonstrate why refusal of a request meets these criteria.

Personal Data Breaches

We have adopted internal procedures for detecting, reporting and investigating a personal data breach.

The reason for this is that the GDPR introduces mandatory breach notification to the Data Protection Authority (the ICO) and in some cases also to affected individuals. Only those breaches which are likely to result in an individual suffering damage will need to be reported e.g. breaches that could result in identity theft or where an individual's confidentiality has been breached. However, even though not all breaches will be subject to mandatory notification, we are still under an obligation to have systems in place to detect and investigate all breaches. We will also maintain an internal breach register.

Where we detect a breach, which is subject to the mandatory reporting rules then we must report the breach to the supervisory authority without "undue delay" and not later than 72 hours after becoming aware of it. This could pose significant challenges given that it can take organisations several hours or even days to identify where the breach took place, which individuals have been affected and the data that has been compromised.

Where a breach must be reported to affected individuals, this will have to be done without "undue delay".

Non-compliance can lead to administrative fines* of up to €10,000,000 or in the case of an undertaking, up to 2% of the total worldwide annual turnover or the preceding financial year, whichever is higher.

Children

The GDPR identifies children as "vulnerable individuals" deserving of "special protection". To that end, you need to be aware that the new rules introduce some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data.

The main provision in respect of children is that where information society services are offered directly to a child and the legal ground for processing personal data is consent, then parental consent will be required for children aged under 16. This threshold can also be lowered to 13 by a Member State.

Ultimately though, under 13's can never themselves consent to the processing of their personal data in relation to online services. This rule is subject to certain exceptions such as counselling services.

Data controller would also be required to make reasonable efforts to verify that consent had been provided.

Offline processing of personal data will continue to be subject to the usual Member State rules on capacity to consent.

International Data Transfers

Under current data protection law, in general terms, the rules on data transfers under GDPR are very similar to those under the DPA with some improvements.

Were applicable, we will review and map any flows of personal data outside the EEA, consider what transfer mechanisms are in place and whether these comply with GDPR or not.

Transfers of personal data outside the European Economic Area (EEA) will continue to be restricted under GDPR

We do not send personal data outsider the EEA whether through the use of service providers such as Cloud Service Providers, bulk emailing services, web hosting services or simply communicating with agents overseas.

The GDPR will continue to offer existing methods of transferring personal data. For example, standard model contract clauses which have been approved by the EU Commission and adopted by a Member States supervisory authority will remain a practical option for most types of transfers and the existing sets of clauses will remain in force. There will also continue to be a set of derogations (exemptions) which will permit the transfer of personal data under certain circumstances e.g. explicit consent and contractual necessity etc.

Breach of the GDPR's rules on data transfers will be subject to maximum level fines of up to 4% of worldwide annual turnover.

Approved By: Sadaf Khan, Pranvera Breshanaj, Pranvera Breshanaj
Date Published: 23/04/2020