Staffcraft Ltd.

hrinpractice

PEOPLE SOLUTIONS FOR PRIMARY CARE

GDPR Overview

Contents

Introduction

This guidance note has been prepared to provide a brief summary of the key aspects and requirements of the new GDPR which is coming into force on 25 May 2018. It should be read in conjunction with the other material created jointly by Staffcraft Ltd., and HRinPractice Ltd., and accessible from our shared GDPR web page - https://www.staffcraft.co.uk/gdpr

Definitions

The GDPR will place obligations on 'data controllers' and 'data processors'. The 'controller' determines the purposes and means of processing the data; the 'processor' is responsible for processing personal data on behalf of the controller.

'Personal data' is any information relating to an identifiable person ('data subject') who can be directly or indirectly identified by reference to that information and, under GDPR, will include location data or an online identifier e.g. an IP address. In HR terms, data subjects will be an organisation's employees, workers, contractors and the family and friends whose data is collected in connection with these contractual relationships (such as emergency contacts and social media connections).

Data known as 'sensitive data' under existing definitions is known under GDPR as 'special categories of personal data', including genetic, health and biometric data but not data relating to criminal convictions.

GDPR covers data which is kept by automated means and manual filing systems where personal data are accessible according to specific criteria, potentially including information ordered according to its chronology.

Individual rights

Data subjects have the following rights regarding their personal data under the GDPR:

The right to be informed

Individuals should receive certain information about the processing of their data, such as the categories of data and the purpose of processing. The information must be concise, transparent and written in clear and plain language. A fee cannot be charged for providing this.

The right of access

Individuals have the right to access their personal data and other supplementary information. A fee can only be charged in certain circumstances (see Access to data)

The right to rectification

Individuals have the right to rectify their personal data if it is inaccurate or incomplete. A request for rectification must be responded to within 1 month, or 3 months if the request is complex.

The right to erase or "the right to be forgotten"

Individuals can request removal or deletion of personal data where there is no compelling reason to keep processing the data. This includes where consent is withdrawn.

The right to restrict processing

Individuals have the right to restrict or block processing of personal data in specific circumstances, including where the accuracy of the data is questioned. The personal data can continue to be stored but no further processing can take place.

The right to data portability

Individuals can obtain their personal data for personal use across different services. A fee cannot be charged and requests must be responded to without delay and within 1 month, or 3 months if the request is complex.

The right to object

Individuals have the right to object to the processing of personal data in specific circumstances, including for processing on the basis of a legitimate interest or direct marketing.

Rights in relation to automated decision making and profiling

Individuals have rights regarding decisions made without human intervention that have a significant effect on the individual. This right does not apply to all automated decisions, including where these are authorised by law.

Data protection principles

There are six data protection principles under GDPR rather than the eight existing ones (See Data Protection). The principles under the GDPR are that data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and,
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Lawful basis for processing

Personal data can only be processed where there is a lawful basis to do so and organisations must determine the lawful basis before processing begins. The appropriate lawful bases needs to be identified in certain pieces of documentation as a result of a data subject's right to be informed, e.g. in privacy notices and responses to subject access requests. There are six lawful bases:

1. Consent
2. Legitimate interests
3. Performance of a contract
4. Legal obligation
5. Vital interests
6. Public task

Consent

Unless another lawful basis applies, organisations generally currently use that of consent to process the data of their employees. However, the rules on obtaining consent are much more stringent under GDPR than under current rules.

Consent must be freely given, informed and unambiguous. It requires positive opt in meaning that organisations cannot use default methods including pre-checked boxes; individuals must be given detailed information on what their consent is being obtained for; the types of processing activity and the name of the controller. Blanket consent to cover many different aspects of processing will not be sufficient.

Documents used to obtain consent should be separate from other terms and conditions in order to ensure data subjects are acutely aware of the consequences of their actions.

Data subjects must be informed of their right to withdraw their consent at any time and there must be no repercussions from withdrawal.

The ICO recognises that the free giving of consent may be compromised by the employer-employee relationship: Employers are in a position of power over individuals and employees may feel they have no choice but to provide consent in order to gain or continue employment. For this reason it is strongly recommended that consent is used as the lawful basis for processing only where all other possible bases are inappropriate.

Privacy notices

As part of enhanced accountability provisions, organisations will have a general obligation to implement measures to show that data protection is a primary concern in processing activities.

A privacy notice can be used as part of a data protection compliance system. A notice under GDPR needs to be more detailed than under current provisions; the ICO recommends that organisations:

- include concise, transparent, and accessible information on how data is processed;
- write in clear and plain language;
- provide it free of charge.

When the data is obtained directly from the data subject, the GDPR requires the following to be included in a privacy notice:

- identity and contact details of controller and Data Protection Officer (if appropriate);
- the purpose of the processing;
- the legitimate interests of the controller or third party where applicable;
- the categories of personal data;
- recipient or categories of recipient of the personal data;
- details of transfers to third country and safeguards;
- retention period or criteria used to determine the retention period;
- the existence of each of the data subject's rights;
- the right to withdraw consent at any time;
- the right to lodge complaints with a supervisory authority;
- the source of the personal data and whether it came from a publicly accessible source;
- the existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

Our new Data Protection Policy and its associated documents incorporate the required privacy notice information. An alternative version is provided by us for recruitment purposes.

Data protection impact assessments

Organisations must, in certain circumstances, carry out a data protection impact assessment to help them identify the most effective way to comply with their data protection obligations.

An impact assessment must be carried out when an organisation:

- uses new technologies; and,
- the processing is likely to result in a high risk to the rights and freedoms of individuals. This can include systematic and extensive processing activities; large scale processing of special categories of data (currently known as 'sensitive' data) or large scale systematic monitoring of public areas.

An impact assessment should include:

- a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an assessment of the risks to individuals;
- the measures in place to address risk, including security and to demonstrate compliance.

It is unlikely that small private sector or charity organisations will undertake activities requiring DPIAs but please check with us if in doubt.

Access to data

Employees have the right to access their data under existing data protection laws and this is known as a subject access request. This right will remain (see Data Protection) under the GDPR but the administrative system will be changed.

Employees have a right to know whether or not their employer is processing personal data about them. If the employer is processing data, the employee has a right to know:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom data has been or will be disclosed;
- the period during which personal data will be retained;
- information on the source of the data;
- information regarding complaints and disputes: the right to complain to a supervisory authority, the right to request rectification or erasure of personal data, to object to processing of data or to restrict that processing; and,
- information on any safeguards where personal data is transferred outside the EEA.

It is a common misconception that employees have a right to see a copy of documents; this is not the case. They have a right see their personal data. However, a request is likely to be most easily dealt with by providing copies of documents. These may need to go through a process of redaction before being sent to avoid the identification of another person.

Organisations have a duty to be fair, transparent, and facilitate the request. Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It can be an offence to alter or erase information to frustrate disclosure.

A request must be complied with without delay - within one month of receipt at the latest (this can be extended by a further two months where requests are complex or numerous but this must be explained to the requester).

Organisations will no longer be able to charge a standard £10 fee for complying with a request. A 'reasonable fee' can be charged only where a request is "manifestly unfounded or excessive, particularly if it is repetitive", or where further copies of the same information is requested.

Refusal to comply with a request is permitted when the request is "manifestly unfounded or excessive". In these circumstances, the requester must be informed without undue delay of the refusal to comply, and within one month at the latest. An organisation's reasons for refusal must be given, together with information on the employee's right to complain to the Information Commissioner or to take legal proceedings.

A subject access request may be refused if the information requested falls into one of the exemptions permitted by the legislation:

- confidential references;
- information that the organisation is required to publish by law;
- personal data processed for the purpose of prevention or detection of crime, the capture or prosecution of offenders and the assessment or collection of tax;
- management planning or management forecasting;
- a record of intentions in negotiations with the employee;
- in relation to core regulatory activities;
- legal privilege;
- health and education records;
- social work records.

Other, less common, exemptions also apply.

An employee may complain to the Information Commissioner if they believe their right of access under the GDPR has been infringed. If the Information Commissioner is clear that an infringement has taken place, it may serve an assessment notice on the employer and has the power to enter the employer's premises, view documents, see the employer's data processing procedures and speak to the workforce. A penalty notice may be served on the employer if an assessment notice is not complied with. The complaint may be escalated to the Information Tribunal if the Information Commissioner fails to deal with the complaint adequately. Courts have the power to make an order for securing compliance if an infringement has occurred.

Data Protection Officer

A new requirement under the GDPR is that organisations must appoint a Data Protection Officer (DPO) where certain criteria are met. Whilst all organisations may choose to have someone with overall responsibility for data security (and we recommend this), it will be a legal requirement only:

- where the organisation is a public authority or body (except for courts acting in their judicial capacity);
- where the core activities of the organisation 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;
- where the organisation carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

In order for organisations to determine if they meet the criteria mentioned above and therefore have a mandatory requirement to appoint a DPO, they will need to interpret key terms such as 'core activities' and 'regular and systematic'. Similarly organisations will need to determine if they are

responsible for processing special categories of data and if they could be considered as a public authority or body.

To assist organisations, the following are definitions of the key terms as provided by both the GDPR and the European advisory body responsible for data protection and privacy, known as Article 29 Working Party (WP29).

“Public authority or body” - a public authority or body is considered as one that is governed by national law. This concept is however not limited to national, regional and local authorities as under the respective national laws this may also include a range of other bodies that are governed by public law.

“Core activities” - these are described as the key operations necessary to achieve the controllers or processors goals.

“Regular and systematic monitoring” - Regular is defined as: (i) ongoing or occurring at particular intervals for a particular period, or (ii) recurring or repeated at fixed times, or (iii) constantly or periodically taking place.

“Systematic” is defined as: (i) occurring according to a system, or (ii) pre-arranged, organised or methodical, or (iii) taking place as part of a general plan for data collection, or (iv) carried out as part of a strategy. Examples of activities that may constitute regular and systematic monitoring include email retargeting, data-driven marketing, profiling and scoring for purposes of risk assessment for detection of money-laundering.

“Special categories of data” - these consist of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The DPO can be an existing employee (no specific qualifications are required but the individual should have professional experience and knowledge of data protection law) and one DPO can act for a group of companies. The role must report directly to the highest level of management and must be given adequate resources to carry out the role. He/she should not be dismissed or penalised for undertaking the tasks required by the role. The role may also be contracted out.

It will be the role of the DPO to:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

DPOs are not considered personally responsible in the event of non-compliance with the GDPR. The responsibilities for any breach in GDPR compliance will always remain with the organisation.

Reporting breaches

A personal data breach has a wider definition than simply losing data. It is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may include a hacking attack or human error e.g. sending information to the wrong email address.

Reportable breaches must be reported to the relevant supervisory authority without undue delay and within 72 hours of discovery. Organisations will be permitted to provide information on the breach in phases where a full investigation is not possible within that timeframe.

A reportable breach is one which is likely to result in a risk to people's rights and freedoms. If this is not a likely consequence, the breach does not need to be reported.

If there is a high risk to people's rights and freedoms, the affected individual(s) will also need to be notified. This may be, for example, where an individual may be discriminated against, suffer financial loss or detriment to reputation or other social or economic disadvantage. Where the breach is such that the public need to be informed, this should be done without delay.

Fines

A breach of GDPR carries a maximum fine of €20million or (if higher) 4 per cent of the organisation's global turnover.

The guidelines on the application and setting of administrative fines sets out the principles for consistent application of fines for data protection breaches. Specific breaches will not carry a "price tag". Instead an assessment will be made on the individual circumstances of the breach against certain criteria. The following will be assessed:

- the nature, gravity and duration of the infringement including the purpose of the processing, the number of people affected by the breach and the level of damage to their rights;
- the intentional or negligent character of the breach, meaning whether the controller knew of the breach and acted wilfully, or whether there was no intention to cause a breach;
- any action taken to mitigate the damage suffered by data subjects. Organisations should do whatever they can to reduce the consequences of the breach for those concerned;
- the degree of responsibility of the controller or processor taking into account measures implemented by them- e.g. has the organisation implemented measures to follow the principles of design and default?;
- previous infringements or whether the data controller is already on the "radar";
- degree of cooperation with the supervisory authority to remedy the breach;
- the type of personal data affected by the breach;
- whether the data controller notified the breach;
- the controller's adherence to codes of practice and approved certification mechanisms;
- any other aggravating feature of the breach;
- the extent to which the data controller notified the supervisory authority of the breach and its cooperation with that authority subsequent to the breach.

In some cases, organisations may receive a reprimand instead of a fine. This may be, for example, where the breach does not pose a risk to the rights of data subjects - e.g. "a minor infringement" or where the data controller is a natural person and the imposition of a fine would be a disproportionate burden.

Record keeping

The following information must be recorded:

1. name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer);
2. purposes of the processing;

3. description of the categories of individuals and categories of personal data;
4. categories of recipients of personal data;
5. details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
6. retention schedules and;
7. a description of technical and organisational security measures.

Registration with ICO

Unless exempt, all organisations that process personal data are required to register with the ICO. Fees are attached to the registration process: the fee structure will change upon GDPR implementation on 25 May 2018. The new charging structure does not necessarily mean that registration must be renewed on this date. Current registrations will continue to run until expired.