Data Protection Legislation Framework (GDPR)

Darlington Training Solutions

Policy Statement

On the 25th May 2018 the new Data Protection Act 2018, which is based on the General Data Protection Regulations (GDPR) replaces the Data Protection Act 1998 in its entirety. It replaces the existing Data Protection Laws to make them fit for the digital age in which ever increasing personal data is being processed.

The Act sets new standards for protecting personal data. Gives people more control over the use of their data and assists in the preparation for a future outside of the EU.

There are 4 main matters provided for, these are:

- General Data Processing
- Law Enforcement Data processing
- Data Processing for National Security Purposes
- Enforcement

All of the above need to be set in the context of international, national and local data processing systems which are increasingly dependent upon internet usage for exchange and transit of data. The UK must lock into international data protection arrangements, systems and processes and this Act updates and reinforces the mechanism to enable this to take place.

Given the size of the legislation and some of the media hype surrounding its introduction this policy is written in 2 Sections.

Section 1 Overview of the Act.

Section 2 The Policy and templates

Section 1

Overview of the Act.

The Act is structured in 7 parts, each of which covers specific areas. These are:

Part 1: Preliminary

This sets out the parameters of the Act, gives an overview, explains that most processing of personal data is subject to the Act and gives the terms relating to the processing of personal data.

Part 2: General Processing

This supplements the GDPR and sets out a broadly equivalent regime to certain types of processing to which the GDPR does not apply.

Part 3: Law Enforcement Processing

This covers;

- "competent authority"
- meaning of "controller" and "processor"
- data protection principles
- safeguards in regard to archiving and sensitive processing
- rights and access of the data subject, including erasure
- implements the law enforcement directive
- controller and processor duties and obligations
- records
- co-operation with the ICO commissioner
- personal data breaches
- the remedy of such breaches
- position of the data protection officer and their tasks
- transfer of data internationally to particular recipients
- national security considerations
- special processing restrictions and reporting of infringements.

Part 4: Intelligence Services Processing

This covers only data handled by the above e.g. MI5 and MI6 and includes rights of access, automated decisions, rectification and erasure, obligations relating to security and data breaches.

Part 5: The Information Commissioner

This covers

- general functions including publication of Codes of Practice and guidance
- their International role
- their responsibilities in relation to specific Codes of Practice
- consensual audits
- information to be provided to the Commissioner
- confidentiality and privileged communication
- fees for services
- charges payable to the commission
- publications
- Notices from the Commissioner
- reporting to parliament.

Part 6: Enforcement

This covers the new enforcement regime in relation to all forms of Notice issued by the Commissioner

- powers of entry and inspection
- penalty amounts
- appeals
- complaints
- remedies in the court
- offences
- special purpose proceedings.

Part 7: Supplementary and Final Provision.

This covers legal changes which the new Act alters in relation to other legal matters, e.g. Tribunal Procedure rules, definitions, changes to the Data Protection Convention etc. and List of Schedule(s).

As you can see, this Act is a huge piece of legislation. The I.C.O. confirms that many concepts and principles are much the same and businesses already complying with the current law are likely to be already meeting many of the key requirements of the GDPR and the new Act.

The Information Commissioner says the new Act represents a “step change” from previous laws. “It means a change of culture of the organisation. That is not an easy thing to do, and its certainly true that accountability cannot be bolted on: it needs to be a part of the organisations overall systems approach to how it manages and processes personal data”. It’s a change of mindset in regard to data handling, collection and retention.

We need to stop taking personal data for granted, its not a commodity we own: its only ever on loan. Individuals have been given control and we have been given fiduciary duty of care over it!

As an organisation handling personal data on a day to day basis, this policy sets out the requirements of the new Act and how we, as an organisation will meet our legal obligations. Staff awareness and understanding of their responsibilities in regard to the handling, collection and retention of data will be core to the successful embedding of this policy.

Preparation: (The 12 Steps)

In order to comply with the requirements of the Act preparation should include the completion of the 12 steps

- Awareness
- Information we hold
- Communicating privacy information
- Individuals rights
- Subject access requests
- Lawful bases for processing
- Consent
- Children
- Data Breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officers
- International Data

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The ICO has issued this guidance as the start of the preparation. They have also made clear that they are aware that for small companies in particular time can be a factor in this preparation, but it is important to remember that you must start the 12 steps in order that you can show compliance

As an organisation we are preparing for this new Act by completing these 12 steps.

Definitions

The GDPR applies to “Controllers”, “Processors” and “Data Protection Officer” and to certain types of information, specifically, “Personal Data” and “Sensitive Personal Data” referred to in the Act as Special Categories of Personal Data”.

“Controllers”

This role determines, on behalf of the organisation, the purposes and means of processing personal data.

“Processors”

This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations on you, e.g. you are required to keep and maintain records of personal data and processing activities. This role has legal liabilities if they are responsible for any breach.

Data Protection Officer**.**

This role is a must only in certain circumstances if you are:

- A public authority (except for courts)
- Carry out large scale systematic monitoring of individuals e.g. online behaviour tracking, or
- Carry out large scale processing of special categories of data, or data relating to criminal convictions and offences e.g. Police, DBS Bodies, Prison Service etc. P33

“Personal Data”

This means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. So, this would include name, reference or identification number, location data or online identifier. This reflects changes in technology which incorporates a wide range of different identifiers. Personal Data applies to both automated and manual filing systems. It can also apply to pseudonymised e.g. key-coded can fall within the GDPR dependent on how difficult it is to attribute the pseudonym to a particular individual. Race, ethnic origin, politics, religion, trade union membership, sex life or sexual orientation.

“Special Categories of personal Data”

This category of data is more sensitive and much more protected. Sensitive personal data specifically includes genetic data, biometric data, health, race, ethnic origin, politics, religion, trade union membership, sexual orientation Safeguards apply to other type of data e.g. criminal convictions and offences; intelligence data etc.

Data Protection Principles

The GDPR sets out the following principles for which organisations are responsible and must meet. These require that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and where necessary, kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR (the safeguards) in order to safeguard the rights and freedoms of individuals; and
f) 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.

“The controller shall be responsible for, and be able to demonstrate, compliance with the principles” Article 5 (2) GDPR

“Lawful bases” for processing

There are 6 lawful bases for processing data. These are:

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital Interests:** the processing is necessary to protect someone’s life.
- **Public Task:** the processing is necessary for us to perform a task in the public interest, or for official functions and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (Does not apply if a public authority is processing data to perform its official tasks).

Consent

The GDPR sets a high standard here. Consent means offering individuals real choice and control. Consent practices and existing paperwork will need to be refreshed and meet specific requirements. These are:

- Positive opt-in, no pre-ticked boxes or other method of “default” consent
- A clear and specific statement of consent
- Vague or blanket consent is not enough
- Keep consent requests separate from other terms and conditions
- Keep evidence of consent – who, when, how, and what you told people
- Keep consent under review
- Avoid making consent to processing pre-condition to any service
- Employers need to take extra care to evidence that consent is freely given, and should avoid over reliance on consent

Consent is one lawful basis to consider but organisations in a position of power over individuals should consider alternative “lawful bases”. If we would still process their personal data without consent, then asking for consent is misleading and inherently unfair.

Legal Obligation

Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulations 2014), which requires us as providers to collect, handle and process data in a prescribed manner.

Legitimate Interests.

- This is the most flexible lawful basis for processing
- It is likely to be appropriate where we process in ways that people would reasonably expect us to, with a minimal privacy impact, or where there is a compelling justification for the processing
- There are 3 elements to consider when using this lawful base. We need to:
- Identify a legitimate interest
- Show that the processing is necessary to achieve it: and balance it against the individual's interests, rights and freedoms
- Legitimate interests can mean ours, interest of third parties, commercial interests, individual or social benefits
- The processing must be necessary
- A balance must be struck between our interests, the individual's and would it be reasonable to expect the processing, or would it cause unnecessary harm, then their interests are likely to override our legitimate interests
- Keep a record of your legitimate interest's assessment (LIA) to help you demonstrate compliance

Contract, Vital Interests or Public Task apply within specific work settings and would be difficult to meet because service providers are subject to specific legislative and regulatory requirements in order to work within a "Regulated Activity".

"Lawful bases" must be determined by the organisation before processing of any personal data and it is vital that thorough consideration is given to this decision.

Individual Rights

The GDPR provides the following rights for individuals:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

All relevant guidance to individual rights is not yet complete, Working Party (WP)29 will continue to work and produce such guidance as is thought appropriate.

Any individual request which falls into the above categories this organisation will follow the relevant guidance currently available on the following website

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/

Privacy notices, transparency and control

To start off a privacy notice, you need to tell people, as a minimum

- who you are
- what you are going to do with their information
- who it will be shared with.

Being transparent, and providing accessible information, is core to compliance and the GDPR. Privacy notices is the most common way to meet the GDPR requirements.

Transparency, in a governance or business context, is honesty and openness and the more transparent we can be the more easily understood and accessible our services become to the people who use them.
In the context of data processing is simply that

“it should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of their personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processor and further information to ensure fair and transparent processing in respect of the confirmation and communication of personal data concerning them which is being processed.”

Information Commissioner: Role and Function.

With regard to the changes within the new GDPR, National Supervising Authorities in all EU member states have had their powers of enforcement enhanced. Our I.C.O. in the UK's supervising authority.

Within the Enforcement Toolbox, the Information Commissioners Office known as the I.C.O., can now issue substantial fines of up to 20 million, or, 4% of an organisation's global turnover for certain data protection infringements. Fines, when appropriate, will be of the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches. The GDPR also empowers the I.C.O. to create tailor made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium sized organisations can take comfort in the fact that they are unlikely to face the sort of punitive fines that rogue tech giants could in order to bring them to head.

Remember: the highest imposed fine limit was £500,000 under the old Act (1998) but the highest fine ever imposed was £400,000 to TalkTalk for failings in connection with a cyber-attack in 2016. The Information Commissioner herself is playing down the "scaremongering because of misconceptions". £20 million fines could put businesses out of business and that is not the intention of the GDPR, though there is a seismic shift in the number of fines that could be imposed. The role and scope of the I.C.O. has not fundamentally changed, but rather has been expanded and enhanced via the new GDPR.

Codes of Conduct and Certification Mechanisms.

Although the use of any of the above is encouraged by the GDPR it is not obligatory. If an approved code of conduct or certification scheme becomes available that covers our processing activity, consideration will be given to working towards such a scheme as a way of demonstrating our compliance.

The I.C.O. will develop its own code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct: DMA Code.

Derogations and Exceptions.

The Act provides that member states of the EU can provide their own national rules in respect of specific processing activities.

All Data Controllers must be familiar with Schedules 1-18 of the GDPR as these are the lawful exemptions pertinent to many other legal frameworks and Acts. These Schedules cover things such as Parliamentary Privilege, Health and Social Work, Criminal Convictions (Additional Safeguards), Research, Statistics and Archiving, Education Child Abuse, and include specific provisions for data processing within the Schedule(s).

For example: Schedule 15: Powers of Entry and Inspection. This Schedule sets out clearly the powers of the Information Commissioner's Office in relation to warrant(s) issued by the courts which allow the I.C.O. to enter premises and inspect data field there, including the seizure of documents. Schedule 18 is where all the legislative changes, in all pertinent primary legislation is found, including the repeal of the Data Protection Act 1998. As the Act is embedded in to the organisation, Data controllers, their role and responsibilities, will need to be reviewed and revised to ensure compliance.

Codes of Practice.

The Act enhances the role of the Information Commission's Office (I.C.O.) in the compilation of such Codes and these will be available in due course. It is important that we are regularly checking the I.C.O. website in order to keep up with current guidance.

Section 2

The Policy

This organisation believes that all data, required for the delivery of the service and the lawful running of the organisation must be collected, handled, maintained and stored in accordance to the requirements of the Data Protection Act 2018.

The General Data Protection Regulations (GDPR) form the basis of the Act but in order to be effective and compliant with its requirements, the Related Policy list should be viewed as core to this policy, as should Section 1 and the Related Guidance links.

PLEASE NOTE All Guidance from the ICO should be considered "Live Documentation" and regularly checked until all Codes of Practice and Guidance are issued. Working Party 29 known as WP29 is a representative body from each of the EU member states who have developed and worked on the Act. WP29 still sits and meets in the European Parliament until all of the complexities of the Act have been clarified and amended into law.

Data Protection Principles

The Act sets out 8 Principles which must be adhered to when processing data

Please refer to the Related Guidance links for further information

The GDPR sets out the following principles for which this organisation is responsible

and must meet. These require that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and where necessary, kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR (the safeguards) in order to safeguard the rights and freedoms of individuals; and
f) 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.

Individual Rights

There are several changes here in particular the Right of Access in relation to timescales and fees. These must be fully understood in relation to anyone submitting a Subject Access request. Please refer to the related Guidance Link

The GDPR provides the following rights for individuals:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Each of the above rights has its own Best Practice Process which you will find here

https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Privacy Notices

This is a new requirement for data processing, it is an accessible information declaration which should set out clearly how we will gather, use handle, store and process personal data.

The Code uses the term “Privacy Notice” to describe all the privacy information that you make available or provide to individuals when you collect information about them. It is often argued that people’s expectations able personal data are changing, particularly through the use of social media, the use of mobile apps and the willingness of the public to share personal information via these platforms.

However, as an organisation we are increasingly aware of the fragile trust which can be easily broken through data breaches and are therefore seeking transparency as a means of building trust and confidence with users of our services. It is the spirit of the Act that privacy, transparency and control become a given for users.

Being transparent by providing a privacy notice is an important part of fair processing. When planning a privacy notice, we need to consider the following:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

The Privacy notice must be easily understood by users of the service and include all of the above, it must also be easily visible so in this organisation it will be displayed

Website, Service user Guide, public office etc.

Privacy and Electronic Communications Regulations (PECR)

This guide issued by the ICO covers specifically electronic marketing messages i.e. phone, fax, email or text, and includes the use of cookies. It introduces specific roles on the above keeping such communication services secure and user’s privacy in regard to traffic and location data, itemised billing, line identification and directory listings

The Data Protection Act 2018 still applies if you are processing personal data. The PECR sets out some extra rules for electronic communications and please be mindful of electronic schedule systems which will also come under PECR

File Retention

The GDPR sets out Guidance on files and retention including archiving, specifically Health and Social Care personal data is generally exempt.

As a provider of services, file and retention guidelines are in place from our Regulator which includes CQC and the NHS as well as Local Authorities via the Service Specification within any contractual arrangements.

A periodic check of the Regulator's Guidance should be part of the review of this policy

Compliance

In order to meet the requirements of the Act a thorough knowledge of the Guidance should be the priority for the Data Controller.

It is also important that the Act is placed in the context of other compliance requirements namely The Health and Social Care Act 2008 (Regulated Activities) (Regulations 2014) and all other lawful requirements such as Regulation 18 Staffing to name but one.

In recognition of the complexities of the Act, the ICO has set up an advice service for small organisations. https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/

Related Guidance

- Smaller Organisations ICO https://ico.org.uk/for-organisations/business/
- Your privacy Notice Checklist https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/your-privacy-notice-checklist/
- Guide to the general data Protection Regulations (GDPR) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Guide to the Privacy and Electronic Communications May 2016 Regulations https://ico.org.uk/media/for-organisations/guide-to-pecr-2-3.pdf
- Records Management Code of Practice for Health and Social Care 2016 https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- ICO Code of practice on privacy notices, transparency and control

  https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

- ICO Data protection Self-Assessment https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

- Direct Marketing Guidance https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

- Data Protection Fees Information Commissioner https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/

- Example of Privacy Notice https://www.johnlewis.com/customer-services/shopping-with-us/privacy-notice

- Guide to privacy and Electronic Communications Regulations (PECR) **https://ico.org.uk/for-organisations/guide-to-pecr/**

Training Statement

All staff must be made aware of the changes to the Data protection Legislation during their Induction. All relevant identified posts must have specific training on the requirements that are now place on organisations. The Data Controller should be responsible for the cascading of any training.

General Data Protection Regulations (GDPR)

Privacy Notice

This privacy notice explains how we use any personal information we collect about you, during the information gathering process known as an Assessment of Need. Topics covered are:

- What information do we collect about you?
- How do we use such information?
- Access to your information and correction

What information do we collect about you?

The nature of our service means that very personal and sensitive information is discussed, openly and honestly, in order to ensure we can meet your health and social care needs in ways that are unique to your individual circumstances. The specific type of information is required in order for us to meet our legal and regulatory obligations as a registered provider.

The Lawful Bases which we use are contained within the Data Protection Act 2018 and is:

Legal Obligation

Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulations 2014), which requires us as a provider to collect, handle and process data in a prescribed manner.

The essential Data we collect from you is:

NAMES

A SIGNATURE CONFIRMING WE CAN ACT FOR YOU

CONTACT TELEPHONE NUMBERS

CURRENT RESIDENTIAL ADDRESS & POST CODE

D.O.B.

CERTAIN HEALTH, MEDICAL AND MOBILITY DETAILS

How information about you will be used.

We may share information regarding your care with those who have a need to know, namely Health Professionals, such as GP's, District Nurses, Hospitals etc., Local Authorities, includes departments such as Social Services, Housing, Day Centres etc. Any relevant person identified by you, such as an L.P.A., and our staff. We would like to contact you about the services we provide, please indicate below your preferred contact method.

Post Email Phone SMS

We will not share your information with anyone except those indicated above, unless required by law. If you do not wish this information to be shared, please indicate below.

Yes No

Personal information supplied to us is used in a number of ways, for example.

- To agree a Care Plan
- To review your care needs
- To monitor your medication
- To help us improve our services

How will we use this information?

Upon completion of your Assessment of Need, we compile a Care Plan which sets out tasks, aspirations and outcomes in order to meet all your identified needs and this is regularly reviewed and updated. This includes liaison with all those involved in your care such as family, your representative relevant health and social care colleagues and other professionals.

Access to your information and corrections.

All files held in your name are available for your perusal and you can ask us to remove information which is inaccurate. Please email or write to us at (Insert contact details here). Where you use our website, cookies are text files which collect log on information and visitor behaviour information. Cookies track visitor use and compile statistical reports on website activity. You can set your browser to accept or decline cookies. Please be aware that a decline preference may mean a loss of function in some of our website features.

For further information on cookies visit: www.aboutcookies.org or www.allaboutcookies.org