Griffiths & Armour

DATA PROTECTION

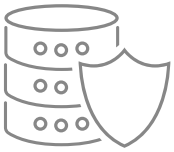
RISK DIRECTORY 2021/2022

DATA PROTECTION
RISK DIRECTORY 2021/2022
INTRODUCTION

In a climate of increased legal duties, raised public awareness and extensive media coverage, data protection has never had such a high profile. Recent well-publicised breaches of data protection have reportedly occurred due to:

- Data being used for purposes outside of the scope of the original intention
- Poor IT system and website security
- Data not being encrypted at rest or in transit
- Loss or theft of portable devices and portable storage media
- Social engineering
- Employee error or fraud
- Postal issues

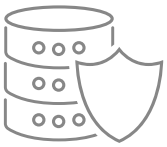
When such an incident occurs, the consequences can include legal action, fines, damage to reputation and loss of business. This guidance seeks to provide an overview of the key legislation in this area, namely:



THE GENERAL DATA PROTECTION REGULATION

THE DATA PROTECTION ACT 2018

GENERAL DATA PROTECTION REGULATION (GDPR)



The GDPR applies to both Controllers and Processors of personal data. Controllers determine the purposes and means of processing data, which is then undertaken by the Processor. Personal data is any data relating to a person that can be identified (either directly or indirectly).

DATA PROTECTION PRINCIPLES

The main data protection principles enshrined within the GDPR require personal data to be:

a) *processed lawfully, fairly and in a transparent manner in relation to individuals;*

b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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 to ensure that personal data that are 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 periods insofar 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 implementation of the appropriate technical and organisational measures required by the GDPR 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.*

Article 5 (i) General Data Protection Regulations

The GDPR requires organisations to be able to demonstrate compliance with the above. Failure to comply with the GDPR can result in maximum fines of €20m or 4% of group worldwide turnover whichever is greater.

LAWFUL BASIS

The GDPR requires organisations to have a valid lawful basis to process personal data. There are six categories of lawful bases and these may be summarised as follows:

CONSENT

Requires positive opt in, i.e. not via the use of pre-ticked boxes or any other method of default consent. Consent should be kept separate from other terms and conditions and not made a pre-condition of a service. It should also be easy for individuals to withdraw their consent. Explicit consent should be accompanied by a clear statement of consent.

CONTRACT

Applies when organisations need to process an individual's data in order to fulfil contractual obligations to them, or because an individual has requested the organisation undertake an activity before entering into a contract.

LEGAL OBLIGATION

Applies when organisations need to process an individual's data in order to comply with a common law or statutory requirement.

VITAL INTERESTS

Relates to the processing of data that is required to protect someone's life.

PUBLIC TASK

Refers to the processing of personal data 'in the exercise of official authority', such as public functions and powers that are set out in law, or to perform a specific task in the public interest that is set out in law.

LEGITIMATE INTERESTS

Likely to apply where individual's data is used in ways they would reasonably expect and which will have a minimal privacy impact, or where there is a compelling justification for the processing. The processing must be balanced against the individual's interests, rights and freedoms. In most instances this will be the lawful basis with which organisations provide personal information to support their insurance arrangements.

Most lawful bases require that any processing undertaken must be necessary.
Organisations should maintain records relating to the lawful basis under which data is processed. This should include individual records of consent and decisions / reasoning behind using a specific lawful basis.

Additional requirements apply to the processing of special category data, data on children and personal data covering criminal offences as follows:

Special Category Data

Examples of special category data include: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics; health; sex life; or sexual orientation. In order to process special category data one of ten conditions must also be met. The ten conditions are available to view, **here**.

Data on Children

Guidance on requirements relating to the processing of data on children is available, **here.**

Criminal Offence Data

Guidance on requirements relating to the processing of criminal offence data is available, **here.**

THE RIGHTS OF INDIVIDUALS

The GDPR provides individuals with the following rights:

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

It is recommended that organisations document policies and procedures to ensure that all these areas are appropriately managed. For the most part, when an individual makes a request in accordance with these rights, organisations have one month in which to respond.
Any action taken should be provided to individuals free of charge unless the request is manifestly unfounded or excessive. The rights of individuals are now considered in turn.

INFORMED

Individuals have the right to be informed about the collection and use of their personal data.
In most cases organisations must provide individuals with privacy information including the purpose of processing their personal information, retention period(s) for this data and who it will be shared with. This is usually achieved via a privacy notice or statement, which should be provided to individuals at the time their data is collected.

ACCESS

Individuals have the right to access their personal data and supplementary information, typically the information that should be provided in the privacy notice/statement.

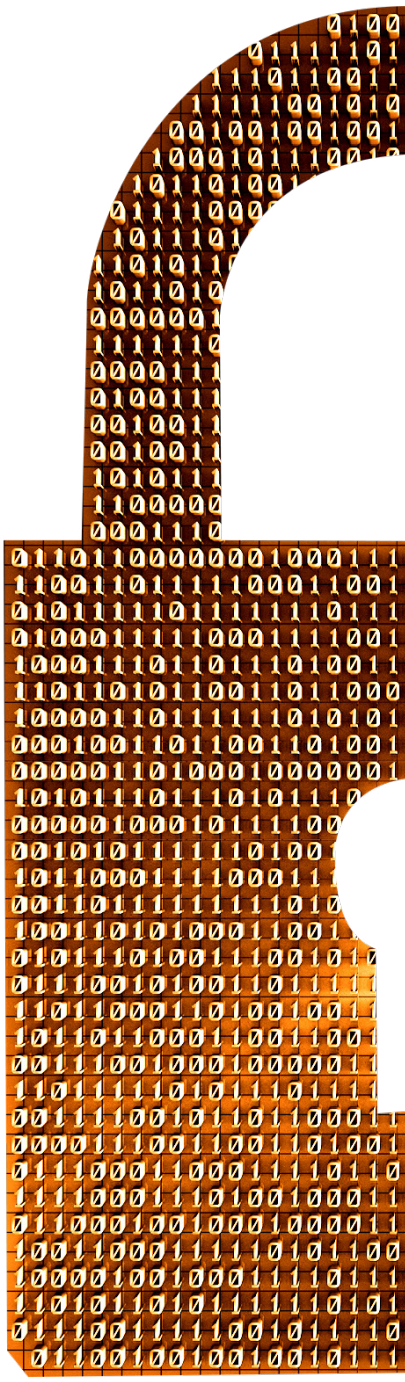
RECTIFICATION

Individuals have the right to have any inaccurate or incomplete personal data rectified.

ERASURE

Individuals have the right to have their personal data erased, otherwise referred to as 'the right to be forgotten'. This right only applies in the following circumstances:

- The personal data is no longer necessary for the purpose for which it was originally collected or processed
- Consent is the lawful basis for holding the data, and this is withdrawn
- The individual objects to the processing of their data where legitimate interests is the lawful basis, and there is no overriding legitimate interest to continue this processing
- The personal data is being processed for direct marketing purposes and the individual objects
- The personal data has been processed unlawfully
- It needs to be erased to comply with a legal obligation
- The personal data has been processed to offer 'information society services' to a child



RESTRICT PROCESSING

Individuals have the right to request the restriction of the processing of their personal data. This right only applies in the following circumstances:

- An individual contests the accuracy of their personal data and this is being verified
- The data has been unlawfully processed and the individual opposes erasure and therefore requests restriction instead
- The personal data is no longer required by the organisation but the individual requires this to be retained in order to establish, exercise or defend a legal claim
- The individual has objected to the processing of their data and the organisation is considering whether their legitimate grounds override those of the individual

PORTABILITY

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It should allow them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.

The right to data portability only applies:

- To personal data an individual has provided to a Controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

OBJECTIONS

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest or exercise of an official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics

PROFILING IS DEFINED AS:

'ANY FORM OF AUTOMATED PROCESSING OF PERSONAL DATA CONSISTING OF THE USE OF PERSONAL DATA TO EVALUATE CERTAIN PERSONAL ASPECTS RELATING TO A NATURAL PERSON, IN PARTICULAR TO ANALYSE OR PREDICT ASPECTS CONCERNING THAT NATURAL PERSON'S PERFORMANCE AT WORK, ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS, RELIABILITY, BEHAVIOUR, LOCATION OR MOVEMENTS.'

Individuals should be notified of their right to object 'at the point of first communication'.

AUTOMATED DECISION MAKING AND PROFILING

Where organisations undertake automated decision making and/or profiling, their obligations include:

- Providing individuals with information about the processing
- Introducing simple ways that individuals can request human intervention or challenge a decision
- Undertaking regular checks to ensure systems are working as intended

Organisations may only undertake automated decision making where the decision is:

- Necessary for the entry into or performance of a contract
- Authorised by the European Union or UK's law applicable to the Controller
- Based upon the individual's explicit consent

OTHER GDPR REQUIREMENTS

Other areas covered by the GDPR include:

- Contracts
- Documentation
- Data protection impact assessments
- Data protection officers
- International transfers
- Security
- Personal data breaches

These are now considered in turn.

CONTRACTS

Controllers are required to have a contract in place each time they use a Processor. Such contracts are required to include specific details and terms, further information on which is available, **here**.

DOCUMENTATION

The GDPR requires both Controllers and Processors to maintain records in several areas and make this available to the Information Commissioner's Office (ICO) upon their request. Further information on the documentation required is available, **here**.

DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) is a process to systematically analyse an organisation's processing and to identify and minimise data protection risks. The GDPR requires organisations to undertake a DPIA if they plan to:

- Use systematic and extensive profiling with significant effects
- Process special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale

It should be noted that the ICO also requires organisations to conduct a DPIA where they plan to:

- Use new technologies
- Use profiling or special category data to decide on access to services
- Profile individuals on a large scale
- Process biometric or genetic data
- Match data or combine datasets from different sources
- Collect personal data from a source other than the individual without providing them with a privacy notice, otherwise known as 'invisible processing'
- Track individuals' locations or behaviour
- Profile children or target services at them
- Process data that might endanger the individual's physical health or safety in the event of a security breach

DATA PROTECTION OFFICERS

The GDPR requires organisations to appoint a Data Protection Officer (DPO) if:

- They are a public authority (except for courts acting in their judicial capacity)
- Their core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking)
- Their core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences

The role of the DPO should include:

- Informing and advising organisations and their employees regarding obligations to comply with the GDPR and other data protection laws
- Monitoring compliance with the GDPR, other data protection legislation and with the organisation's own data protection policies
- Advising on and monitoring DPIAs
- Co-operating with the ICO and acting as their first point of contact

INTERNATIONAL TRANSFERS

The GDPR imposes restrictions on the transfer of personal data outside of the European Union. Further information is available, **here**.

SECURITY

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Compliance with existing data security standards such as ISO27001 or the government-backed Cyber Essentials scheme can assist in this regard. Further information on good cyber security practice is also available from Griffiths & Armour upon request.

PERSONAL DATA BREACHES

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Organisations must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. A notifiable breach is one where it is likely to infringe on individuals' rights and freedoms, which requires assessment by the organisation. Where organisations decide they do not need to report the breach to the ICO, they are required to justify this decision and therefore should document it.

Processors are required to notify Controllers of personal data breaches without undue delay.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR requires organisations to also inform those concerned directly and without undue delay.

DATA PROTECTION ACT 2018

Very much in summary the new Data Protection Act supplements the GDPR by addressing the following areas:

GENERAL DATA PROCESSING

- Applying standards similar to the GDPR to all general data processing
- Providing definitions for terms used in the GDPR in a UK context
- Ensuring that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health, and safeguarding situations can be maintained
- Specifying the areas where explicit consent would not be required to process special categories of personal data, for example for preventing fraud or insurance purposes
- Providing appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification (including for national security purposes)
- Setting the age from which parental consent is not required to process data online at age 13 (supported by a new age-appropriate design code enforced by the ICO)

LAW ENFORCEMENT PROCESSING

- Providing a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes
- Allowing the unhindered flow of data internationally whilst providing safeguards to protect personal data

NATIONAL SECURITY PROCESSING

- Ensuring that the laws governing the processing of personal data by the intelligence services remain up-to-date and in line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats

REGULATION AND ENFORCEMENT

- Enacting additional powers for the ICO who will continue to regulate and enforce data protection laws
- Allowing the ICO to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches
- Empowering the ICO to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request
- Restoring a wholly domestic basis to the UK's data protection laws whilst allowing continued application of GDPR standards

GRIFFITHS & ARMOUR RISK MANAGEMENT SERVICES

Risk management is a cornerstone of Griffiths & Armour's proposition. Simply put, good quality risk management practices lead to fewer incidents and claims, which in turn help minimise premium spend and retained costs. Our guiding principles for risk management are innovation, practicality and a clear focus on your desired outcomes, which can vary from reductions in premiums to legal compliance. This, coupled with our core belief that you should get the very best we have on offer from day one, ensures a strong partnership based on communication, trust and transparency. Specialisms include:

- STRATEGIC RISKS
- BUSINESS CONTINUITY AND SUPPLY CHAIN
- CYBER RISKS
- ONLINE RISK MANAGEMENT SYSTEMS
- LIABILITY CLAIMS DEFENSIBILITY
- HEALTH, SAFETY AND ENVIRONMENT
- MOTOR FLEET RISK MANAGEMENT
- PROPERTY RISKS

If you would like to discuss any of these risk management services please contact us on 0151 236 5656 or by **email**.

ACKNOWLEDGEMENTS, REFERENCES AND RECOMMENDED FURTHER READING

- Guide to the General Data Protection Regulation (ICO)
- Preparing for the General Data Protection Regulation: 12 Steps to Take Now (ICO)
- Data Protection Self-Assessment Website (ICO):

More information can be found, **here.**

LEGAL NOTICE

Insurance Brokers and Professional Risks are divisions of Griffiths & Armour, a partnership which is authorised and regulated by the Financial Conduct Authority.

Risk management services are not regulated by the Financial Conduct Authority.

This document does not provide legal advice and is not a substitute for obtaining specific legal advice in order to protect the interest of your business. Should you require legal advice on any of these matters, please contact your legal adviser. It is intended only to highlight issues that might be of interest to Griffiths & Armour clients. The contents of this document are based primarily on the legal position under English law and may be subject to change. Further, more detailed advice may be appropriate in relation to other jurisdictions in which you work. Where links to third party websites are provided, we accept no responsibility for their content.

OUR VALUES:

SUPPORTIVE

PERSONAL

PROACTIVE

RELIABLE

& that's the difference

griffithsandarmour.com

Assurex GLOBAL

Insurance Brokers Chartered

IB0045