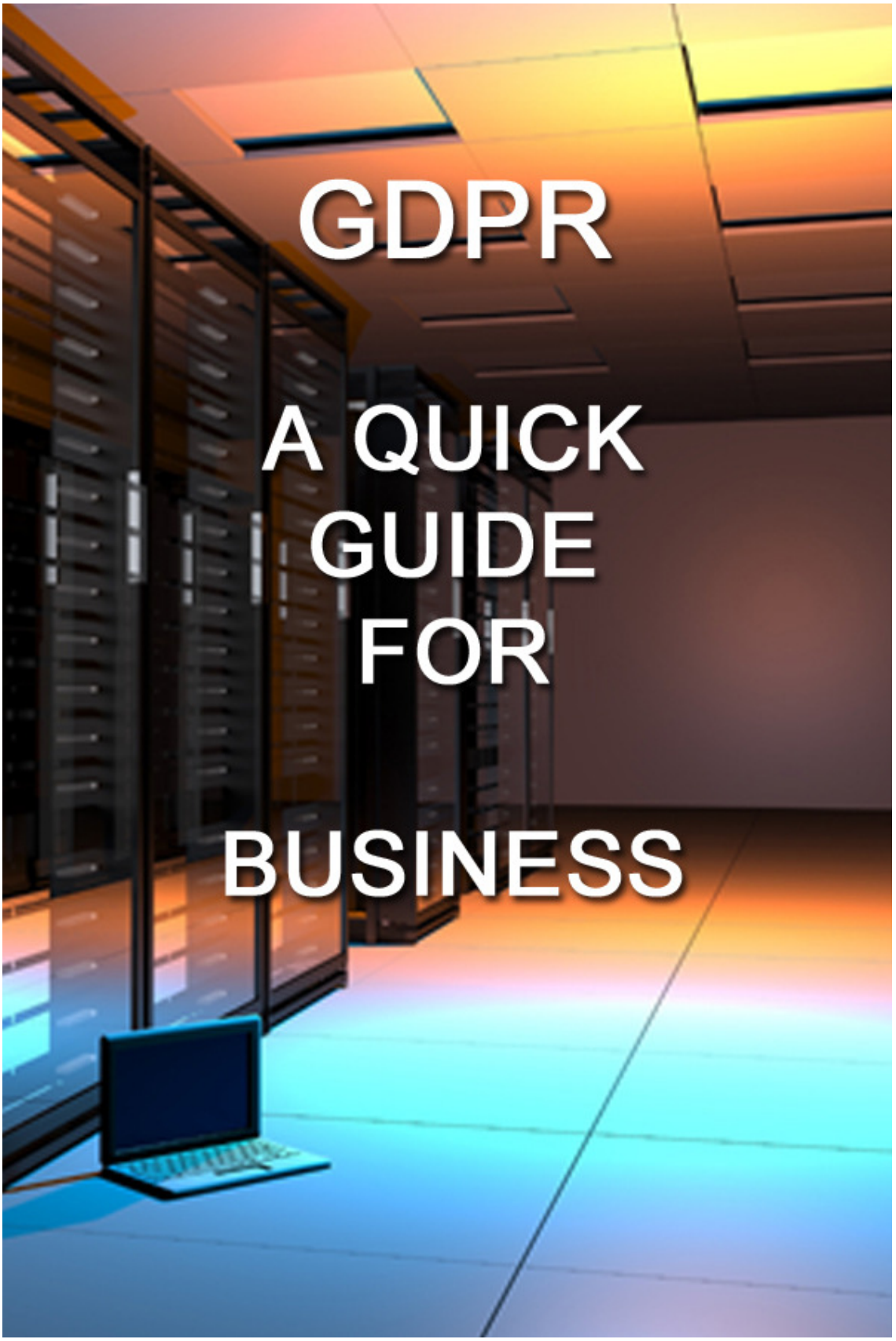
GDPR
A QUICK
GUIDE
FOR
BUSINESS

Legal Notice

While all attempts have been made to verify information provided in this publication, neither the author nor the publisher assumes responsibility for error, omissions or contrary interpretations of the subject matter herein.

This publication is not intended for use as a source of legal or accounting advice.

The purchaser or prospect of this publication assumes responsibility for the use of these materials and information.

The author and publisher assume no responsibility whatsoever on the behalf of any publisher or prospect of these material

Disclaimer

This guide is produced for information purposes only.

It is meant to provide the reader with information and advice relating to GDPR legislation with particular regard to data protection.

The source of information has been provided by documentation published by the Information Commissioner's Office (ICO). The author and publisher of this guide cannot accept any liability for its accuracy. We do not provide this information as a recommendation for implementation and suggest you verify all facts independently.

Contents

Does GDPR apply to you and your company?

It applies to any individual whose responsibility it is to determine the purposes and means of processing personal data and also to anyone who processes personal data on behalf of a controller. So, what that means is if your company processes personal data and you are responsible for it in any way then GDPR applies to you. You could be an individual trader, a company director or employee.

It is the duty of the data controller to ensure the processors and contracts fully comply with GDPR. However, processors of personal data are required by law to keep up to date records of personal data and processing activities. The processor is legally liable to any data process breach.

In effect, all companies in the UK and EU involved in controlling or processing personal data, are affected by GDPR.

What is personal data?

What constitutes personal data, as far as GDPR is concerned, is any information that relates to an identifiable person, and where that information can be used to identify that person. So, email, name and address, an identifying number or reference, an online identifier, and even location are all classed as personal data if it relates to an individual.

In some cases an identifier could be a code or pseudonym, which may fall within the scope of GDPR depending on the level of difficulty in attributing the identifier with the individual.

The rules applicable to GDPR include both automated and manually entered data and to both electronic and manual storage records and systems.

Processing personal data

Are you lawfully processing personal data? The laws states you must determine your lawful basis for processing personal data and then ensure this is fully documented. The lawful basis will have an effect on the individual's personal rights. The extent of this is somewhat determined by whether the individual has given permission for the data to be processed. If they have then their rights to have their data deleted will be that much more significant.

The above is particularly applicable, but not limited to, public authorities and highly regulated sectors.

The importance of consent

It is imperative that consent is fully understood to mean consent given by any individual is not optional but freely consensual.

For example, consent means offering individuals genuine choice and control. It requires positive opt-in and not predetermined options by default, as in pre-ticked boxes.

Consent requests must be clear, specific and precise. Individuals must be made aware that consent can be withdrawn and it must be made clear how. If there is to access to consent by any third party controllers then this must be made clear. All evidence of consent must be kept on record. For example, from who, when, how and what the individual was told about consent. Transparency is paramount and there can be no room for complacency.

Consent data must be reviewed regularly and refreshed if there are any changes. Although consent is not always possible or can sometimes be difficult, then another means of consent, within a lawful basis, may be justified as more appropriate.

Consent checklist

1). Have you checked that consent is the most appropriate lawful basis for processing?

2). Have you made the request for consent prominent and separate from you terms and conditions?

3). Have you asked that individuals actively and positively opt in?

4). Have you ensured you do not use pre-ticked boxes or any kind of consent by default?

5). Have you used plain, easy to understand language in all your verbal, printed and electronic consent request procedures?

6). Have you clearly specified why you want the data and explained what you will be doing with it?

7). Do you give granular options to consent to independent processing operations?

8). Have you clearly named your organisation and any third party controllers who will rely on the consent?

9). Have you explained to the individuals that they are at liberty to withdraw their consent on request?

10). Have you ensured that individuals understand they can refuse to consent without detriment?

11). Have you ensured you have not made consent a precondition of service?

12). Have you ensured that parental consent and age verification measures are in place if offering online services directly to children. (Refers to children aged under 16 or in some cases under 18, and if applicable).

Individual rights

The GDPR makes provision for individual rights including:

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

Individual rights in more detail

The right to be informed means you may have an obligation to provide 'fair processing information'. This typically applies to a privacy notice. It emphasises the need for transparency in how you use or process personal data.

The GDPR sets out what information you should supply and when the individual should be informed. The information you need to supply will depend, to some extent, on how you obtained the data. For example, was it obtained from the individual directly?

GDPR stipulates that the information you supply relating to the processing of personal data must be concise, transparent, easily accessible and intelligible. It must also be written in clear and plain language, particularly if addressed to a child, and it must be free of any charge.

The right to erasure is the right to be forgotten. This means the individual has the right to request deletion of, or the complete removal of any personal data, where there is no genuine reason for its continued reference or processing.

The right to erasure applies to specific circumstances including where the personal data is no longer required, or is necessary in respect of its original purpose, for which it was collected or processed.

It must also be erased should the individual withdraw consent for its continued use or processing. This also applies if the individual objects to the processing of personal data, for which there is no legitimate reason or interest for continued processing.

The right to erasure also applies where personal data was unlawfully processed and in relation to the offer of information concerning a child. Should the processing of personal data be the cause for distress, then the case for erasure is compounded.

The processor can refuse to comply with a request for erasure if it can be proven that the personal data is required for the right of freedom of expression and the freedom of information. This right to refusal also covers situations, where the personal data is required to comply with a legal obligation or is required by an official authority in relation to a public interest task or performance.

If the personal data is required for public health issues and is in the public interest, or if the personal data is required to be archived in the public interest for scientific or historical research, there may also be a case for refusal.

Refusal is not limited to the above and would also include the exercise or defence of legal claims, and for use in evidence in a court of law.

The right to object means individuals can object to the processing of personal data if the data is to be used in the performance of a task in the public interest of official authority, which includes profiling. This aspect also includes for purpose of scientific or historical research and statistics.

If you process personal data for the performance of a legal task or in the interests of an organisation the individuals must have an objection on the grounds relating to their particular situation. Personal data can be continued to be processed if you can demonstrate legitimate grounds for processing.

This might include overriding the interests, freedoms and rights of the individual if it can be established that the personal data is required for the defence of legal claims. Individuals must be informed of their rights to object at the point of first communication. It must also be stated in your privacy notice.

If you process personal data for direct marketing purposes then you must stop processing the data immediately you receive and objection. In this particular case there are no exemptions and no legitimate grounds for refusal.

No fees can be charged for the cessation of processing personal data due to an objection. The right to object must be brought to the attention of the individual at the point of first communication and in your privacy notice.

You are not required to comply with an objection if you are conducting research, which involves the processing of personal data for the performance of a public interest task.

The right to access means individuals have the right to be aware of and to access their personal data together with any relevant supplementary information. The individual also has the right to verify the lawfulness of the data processing relating to them.

Under GDPR, the individuals are entitled to obtain confirmation that their data is being processed, and be able to access any information, which corresponds to that which is mentioned in a privacy notice.

On request you must provide a copy of any information held on an individual for processing purposes, and provide this free of charge. A reasonable fee, covering administrative costs, can be charged for repetitive requests for information or requests that are proven unfounded or excessive.

Any requests for information must be complied with at the earliest possible opportunity and at the very latest, one month after receipt. Should requests be of a complex nature or numerous then the period of compliance can be extended by a further 2 months. However, if this is the case then individuals must be informed of the reason for the extension.

If you refuse to respond to the request for the provision of information then you must explain your reasons to the individual and inform them of their rights to complain.

The right to restrict processing means individuals have a right to suppress, restrict or block processing of personal data. Where the individual has exercised their right to restriction, you are permitted to store the minimum of data but refrain from any further processing.

You must restrict processing where the individual has contested the accuracy of the personal data, until the data has been verified. You should also restrict the processing of data should any concerns arise relating to the purpose for processing unless it is necessary for the performance of a public task or for legitimate legal interests.

Procedures need to be reviewed in order to establish where you are required to restrict the processing of personal, data. If data has been disclosed to third parties then you must inform them about the restriction of the processing, if it is reasonably practicable to do so.

The right to rectification means the individual has the right to have their personal data rectified, due to inaccuracies or if incomplete.

Where personal data may have been disclosed to third parties then you must inform them of the rectification as soon as is practicable. Individuals concerned must also be informed of the disclosure to third parties, where appropriate.

All requests for rectification must be complied with, within one month. This period can be extend to two months where the request for rectification is complex. If for any reason you are not taking action on a request for rectification then you must inform the individual of their right to complain. Complaints can be made to a supervisory authority.

The right to data portability means individuals have the right to view, obtain and reuse their personal data for their own purposes. They are permitted to move, copy and transfer personal data electronically without hindrance.

This right allows individuals to take advantage of consumer offers and services and to better understand their spending or shopping habits. It is applicable based on the individual's consent or for the performance of a contract, processed manually or automatically.

To comply with this individual right, you must provide the personal data in a structured form, which is machine readable. This means structured so that software can extract specific elements of the data. This can include open formats or CSV files enabling other organisations to use the data.

On request by the individual, you are required to transmit the personal data to another organisation, if you have the means to do so. You cannot charge a fee for this service.

Rights relating to automated decision making and profiling means GDPR provides safeguards against risk that a potentially damaging decision is taken without human intervention.

Automated decision making operations need to be reviewed to ensure the individual is protected under the requirements of GDPR. Individuals have the right not to be subject to any such decision if it is based on an automated process, which could have a legal effect on the individual.

You must ensure individuals are adequately able to obtain or request human intervention and allowed to express their point of view. Also, they must be permitted to obtain an explanation of any decisions so that they are able to challenge it.

These rights do not apply to circumstances, in which the individual enters into a contract with you or is authorised by law or is based on explicit consent.

Profiling is defined as any form of automated processing intended to evaluate specific aspects of an individual in order to analyse for example, personal health, economic situation or performance at work. It might also include the analysis of behaviour, reliability, personal preferences, location and movements.

You are required to ensure that processing is fair and transparent. You must provide meaningful and easily digestible information about the logic involved in collecting such data, together with its significance and possible consequences.

Appropriate mathematical and, or statistical procedures must be used for profiling and you must implement technical and organisational measures to enable inaccuracies to be determined and corrected for the purpose of risk reduction.

You must not rely on automated decisions for any purpose concerning that of a child and, or be based on the processing of special categories of data unless the processing is necessary for reasons of substantial public interest base on state law.

You must provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Accountability & Governance

The GDPR includes provisions that promote accountability and governance to compliment the requirements relating to the significance of transparency.

In certain circumstances you are legally required to put into place comprehensive governance measures including privacy impact assessments and privacy by design. These measures are intended to minimise the risk of breaches and to further protect personal data.

The accountability principle means that you can unequivocally demonstrate that you comply with the principles and states that this is your responsibility. Demonstrating that you comply means implementing measures to ensure internal data protection policies, such as staff training, audits of processing activities, and reviews of internal HR policies.

You must maintain relevant documentation on processing activities and where appropriate appoint or nominate a data protection officer.

Contracts

A controller is liable for the compliance of GDPR and therefore must ensure that any contract between them and a data processor is entered into with the understanding of each other's responsibilities and liabilities.

The GDPR sets out what must be included in the contract. Processors must provide controllers with guarantees that the requirements of the GDPR will be met and all the rights of individual data subjects will be adequately protected.

Both controllers and processors are subject to fines for no compliance of GDPR, so it is in the interest of both parties to ensure there are documented instructions and agreements in place to ensure all those concerned or connected with data processing procedures, meet their obligations and responsibilities.

Contracts must address:

- The subject matter and duration of processing
- The nature and purpose of the processing
- The type of personal data and categories of the subject
- The obligations and rights of the controller

The processors responsibilities include:

- To only act on written instructions from the controller
- To not use a sub-processor without the written authorisation of the controller
- To co-operate with supervisory authorities as required
- To ensure the security of its processing procedures
- To notify the controller of any personal data breaches

Documentation & Records

Together with the obligation to provide comprehensive and transparent privacy policies, if your organisation employs more than 250 employees, you must maintain internal records of processing activities.

For organisations with less than 250 employees you are required to maintain records of activities relating to higher risk processing such as, a risk to the rights and freedoms of the individual and, or processing special categories of data, criminal convictions and offences.

You need to record the name and details of your organisation and that of controllers and data protection officer(s). You need to specify the purposes of the processing and the description of any categories of individuals and categories of data processed.

You need to record retention schedules and descriptions of technical and organisational security measures. You may at any time be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Data protection by design and default

This refers to the GDPR in respect of your general obligations to implement technical and organisational measures. These measures must show that have considered and integrate data protection into your general processing activities.

Organisations should refer to the documentation provided by the ICO in relation to data protection, which will suffice until such time as the provisions of GDPR is updated to reflect these changes.

Follow this link: https://ico.org.uk/for-organisations/guide-to-data-protection/

Data protection impact assessments

DPIAs help organisations to determine the most effective ways to comply with data protection obligations and to meet individual's expectations in relation to privacy.

Data Protection Impact Assessments are basically a means for identifying potential problems and to providing fix solutions at an early stage. This can help reduce costs and limit any potential damage to reputation, which might otherwise occur.

You need to conduct a DPIA when adopting new technologies and when processing could result in in high risk to the rights and freedoms of individuals. This could include extensive data processing activities, profiling and where decisions have possible legal effects on individuals.

You would also need to conduct a DPIA where large scale processing of special categories of data are concerned, relating to criminal offences and convictions.

The DPIA should contain information relating to descriptions of processing operations and the purposes. This includes any legitimate interests and pursuits of the data controller.

It should also contain an assessment of the necessity to process the data in relation to the purpose and an assessment of the risks to the individuals. It should include measures in place to address risk, in terms of security, and to demonstrate that you comply.

Data Protection Officers

It is a requirement of the GDPR that organisations appoint or nominate a Data Protection Officer, in some cases.

A Data Protection officer must be appointed if you are a public authority or carry out large scale systematic monitoring of individuals, such as online behaviour tracking. It also applies to organisations that carry out large scale processing of special categories of data relating to criminal convictions of offences.

Taking into account organisational size and structure, you are permitted to appoint one DPO responsible for a group of companies or a group of public authorities. If you appoint a DPO you must ensure they are competent and fully conversant with all aspects relating to GDPR compliance.

The duties of the DPO include informing and advising the organisation and its employees about their obligations to comply with the GDPR. It also includes monitoring compliance and that of other data protection laws. Managing internal data protection and analysis, and impact assessments are also part of the duties together with staff training and internal audits.

The DPO must report directly to the highest management level (board level) and must operate independently, without dismissal or otherwise penalised for performing the required tasks.

Codes of conduct and certification

Demonstrating that you comply with the rules and obligations of the GDPR, may require that you sign up to an approved code of conduct or certification scheme. Although this is not compulsory or obligatory, if you have the opportunity to do so and it covers your processing activity then it would be recommended. This might be of particular interest to micro and small to medium sized enterprises.

Benefits of adhering to a recognised conduct and certification scheme include improved transparency and accountability. This would enable individuals to distinguish between the organisations that meet the GDPR requirements, and shows they can be trusted with their personal data.

Being part of such an organisation that champions codes of conduct and provides certification can provide mitigation against enforcement action and improve standards by establishing best practice.

Codes of conduct and certification can be drawn up by trade associations and other representative bodies. Codes should be prepared in consultation with all major stakeholders including individuals. They must be formally approved by the relevant supervisory authority and must comply fully with the requirements of the GDPR.

Such codes must address fair and transparent data processing and the collection of personal data. It should also address legitimate interests pursued by controllers with regards to specific contexts.

Other requirements of the codes include the pseudonymisation of personal data and information provided to individuals and the exercise of individual's rights. Other topics include the information provided to, and the protection of children, including the mechanisms for obtaining parental consent.

Technical and organisational measures should be addressed together with breach notification, data transfers outside of the EU, and dispute resolution procedures.

Security measures

The GDPR requires personal data to be processed within a secure environment and with regard to the protection against unauthorised or unlawful processing activities. It also requires that data and processing activities are protected against accidental loss or destruction.

Appropriate technical and organisational security measures and procedures must be in place. The ICO has provided guidance to assist organisations with security threats

and data security breach issues. Further guidance will be forthcoming in respect of GDPR regulations and compliance.

Data breaches

It will the duty of all organisations to report certain types of data breach to the relevant supervisory authority. It may be necessary for data breaches to be reported to affected individuals also.

A personal data breach is defined as more than a loss of personal data. It can also mean a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to any personal data.

You must notify the relevant supervisory authority if there is a breach, which constitutes a risk to the rights and freedoms of individuals. This can include damage to reputation, discrimination, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

You must notify the relevant supervisory authority if the breach is likely to expose customer details, leaving individuals open to identity theft. This particular example would require that you also notify the individuals concerned directly.

Further reading:

https://www.eugdpr.org/