etl

www.etlsolutions.com

A REALLY QUICK GUIDE TO THE GDPR

APRIL 2018

1.

The GENERAL DATA PROTECTION REGULATION (GDPR) concerns “the processing of personal data wholly or partly by automated means...” for people in the European Union whether it is processed in the EU or elsewhere.

A note for UK-based individuals and organisations - January 2021:

Although the UK has left the EU, the UK Government has incorporated the provisions of the GDPR into domestic legislation as the UK GDPR. This means that the rules in this guide continue to apply equally in the UK.

Information for this document has been taken from various publications of the Information Commissioner’s Office. While every effort has been taken to ensure that the information is correct, it should be noted that this document is intended as a guide only and is not to be taken as legal advice. For further information please go to www.ico.org.uk.

2.

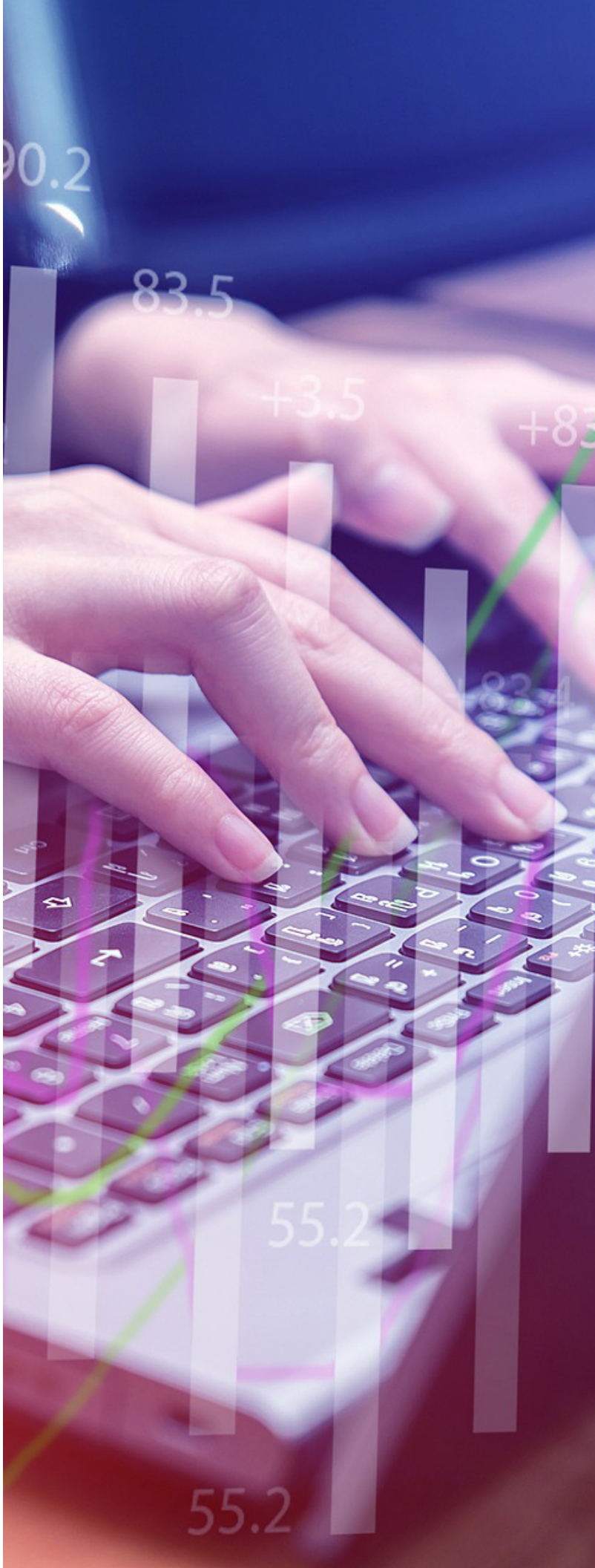
The GDPR applies to:

a. ‘controllers’ and ‘processors’.
A controller determines the purposes and means of processing personal data.
A processor is responsible for processing personal data on behalf of a controller.

b. ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

c. automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

d. sensitive personal data, which is referred to as ‘special categories of personal data’.The special categories specifically in clude genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.



3.

Personal data must 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;

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;

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;

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.

4.

The controller is responsible for, and must be able to demonstrate, compliance with the principles.

5.

There must be a valid lawful basis in order to process personal data:

a. There are six available lawful bases for processing.

b. Most lawful bases require that processing is ‘necessary’.

c. The lawful basis must be determined before the processing is begun, and should be documented.

d. Our privacy notice should include our lawful basis for processing as well as the purposes of the processing.

e. If we are processing special category data we need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

f. If we are processing criminal conviction data or data about offences we need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

6.

The lawful bases for processing are set out in the GDPR. At least one of these must apply whenever personal data is processed:

a. Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

b. Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

c. Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

d. Vital interests: the processing is necessary to protect someone's life.

e. Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

f. 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.

7.

The GDPR sets a high standard for consent. Consent isn't always needed. If consent is difficult, look for a different lawful basis.

a. Consent requires a positive opt-in. Pre-ticked boxes or any other method of default consent must not be used.

b. Explicit consent requires a very clear and specific statement of consent.

c. We must keep our consent requests separate from other terms and conditions.

d. We must be specific and 'granular' so that we get separate consent for separate things. Vague or blanket consent is not enough.

8.

Legitimate interests is the most flexible lawful basis for processing, but we cannot assume it will always be the most appropriate.

a. It is likely to be most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

b. If we choose to rely on legitimate interests, we are taking on extra responsibility for considering and protecting people's rights and interests.

c. There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. 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.

d. The legitimate interests can be our own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

e. The processing must be necessary. If we can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

f. We must balance our interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override our legitimate interests.

g. We should keep a record of our legitimate interests assessment (LIA) to help us demonstrate compliance if required.

h. We must include details of our legitimate interests in our privacy notice.

9.

The GDPR provides the following rights for individuals:

a. Right to be informed
b. Right of access
c. Right to rectification
d. Right to erasure
e. Right to restrict processing
f. Right to data portability
g. Right to object
h. Rights related to automated decision making including profiling.

10.

Whenever a controller uses a processor it needs to have a written contract in place.

a. The contract is important so that both parties understand their responsibilities and liabilities.

b. The GDPR sets out what needs to be included in the contract.

c. Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

d. Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

e. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

11.

In addition to its contractual obligations to the controller, a processor also has the following direct responsibilities:

a. not to use a sub-processor without the prior written authorisation of the data controller;

b. to co-operate with supervisory authorities (such as the ICO);

c. to ensure the security of its processing;

d. to keep records of processing activities;

e. to notify any personal data breaches to the data controller;

f. to employ a data protection officer; and

g. to appoint (in writing) a representative within the EU if needed.

12.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

13.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

14.

There are explicit provisions about documenting our processing activities:

a. We must maintain records on several things such as processing purposes, data sharing and retention.

b. We may be required to make the records available to the ICO on request.

c. Documentation can help us comply with other aspects of the GDPR and improve our data governance.

d. Controllers and processors both have documentation obligations.

e. For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.

f. Information audits or data-mapping exercises can feed into the documentation of our processing activities.

g. Records must be kept in writing.

h. Most organisations will benefit from maintaining their records electronically.

i. Records must be kept up to date and reflect our current processing activities.

15.

Data protection impact assessments (DPIAs) help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

16.

It is a requirement that organisations appoint a data protection officer (DPO) in some circumstances.

The DPO's minimum tasks are:

a. To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

b. To 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.

c. To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

17.

Personal data must be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

18.

The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries or international organisations.

19.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

a. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

b. We should ensure we have robust breach detection, investigation and internal reporting procedures in place.

c. We must also keep a record of any personal data breaches, regardless of whether we are required to notify.

20.

If we are a data processor, and we suffer a breach, we must inform the data controller without undue delay as soon as we become aware.

a. This requirement allows the data controller to take steps to address the breach and meet their breach-reporting obligations under the GDPR.

b. The requirements on breach reporting should be detailed in the contract between the data controller and the processor.