THE NEW GDPR REGULATION
25 MAY 2018

Compiled by: POLLY HEALY

Key Terminology - Key Changes - New Terms

Infringements - Examples of Breaches . How to Avoid Being Compromised
Key Definitions - Seven Key Principles - Accountability - What to do to Comply

<u>Obtaining Consent</u>
Information to Provide to an Individual - Ways to Obtain Consent
Withdrawing Consent - Pre-Existing Consent
Individual's Rights . Right to Review Information - Access Rights
Charges. The Right 'To be Forgotten' - Restricting Processing -

---

<u>Controllers and Processors</u>
Controllers - Data Security - Reporting a Breach-
Processors

The New GDPR Regulation- 25 May 2018

https://ico.org.uk

The aim of the law is to prevent people or organisations from holding and using inaccurate information on individuals, whether relating to private lives or organisations.

This will give the public confidence about the use of their personal information and will also ensure that they have the legal right to check the information being held about them.

It requires organisations to keep personal data safe and secure, and to ensure that it is not misused.

Individuals will have extended rights and businesses have greater responsibilities.

To protect individuals from:
- Identity theft
- Nuisance calls
- Junk mail
- More control over how personal data is used

Breaches of the GDPR are criminal offences and can result in severe penalties.

KEY TERMINOLOGY - Alphabetical

Term	Meaning
(DATA) CONTROLLER	Person (or entity/organisation) determining the purpose and means of processing personal data.
DATA BREACH	Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
DATA SUBJECT	An individual (person) subject of the data. This includes employees.
DPA	Data Protection Authority or Supervisory Authority - eg: ICO
EU-US Privacy Shield	A standard making transfers of data to the US unlawful.
GDPR	General Data Protection Regulation (the law).
PERSONAL DATA	Information relating to an identifiable individual.
PROCESSING	Any operation performed upon personal data.
(DATA) PROCESSOR	Person (or entity) that processes data on behalf of a Controller
SENSITIVE PERSONAL DATA	Data that reveals race or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health and sex life. In most cases, criminal proceedings or convictions are treated as sensitive in addition.
THIRD COUNTRY	A jurisdiction outside of the EEA.

KEY CHANGES

1. New regulations for obtaining consent to collect personal data.
2. The age barrier or 13 to be lifted to 16 for data collection.
3. A requirement to delete data that is not being used for its original purposes.
4. The ability to withdraw consent to data processing.
5. A 72-hour limit to notify breaches to regulators.
6. Large data controllers must appoint a Data Protection Officer.
7. Fines of up to Euros 20,000,000 or 4% of global group annual income.
8. The single Supervisory Authority will be the ICO.

NEW TERMS

Personal Data Breach:

A new term leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Consent of the individual:

Only expressed consent will be allowed and implied consent will no longer apply. Organisations will need to amend their 'terms of business' in order to comply with this requirement.

Right to be forgotten:

This is when consent is withdrawn, organisations are required to erase personal data, and request that any third party, with which this information has been shared, do likewise.

This has far-reaching implications where processing is outsourced and where data is shared.

INFRINGEMENTS

When looking at infringements, the ICO will take into account:

1. The nature, gravity and duration of the infringement.
2. The number of individuals affected.
3. Any elements of intentional behaviour or negligence.
4. Any mitigating steps taken.
5. Any previous infringements.
6. The degree of co-operation.
7. Self-reporting.
8. Any aggravating or mitigating circumstances.

The ICO is required to impose sanctions which are effective, proportionate and dissuasive.

EXAMPLES OF BREACHES OF DATA PROTECTION

- 2007 - Some major high street Banks were named and shamed for leaving customers' personal information in unsecured rubbish bins outside their premises.
- 2010, a Council was fined when they inadvertently sent details of an offender to a member of the public, by fax, instead to a barrister.
- 2010 - A company was find for allowing an employee to take home an un-encrypted laptop containing customers' personal data.
- 2013 - The Ministry of Justice was fined after an email was inadvertently sent with a spreadsheet attachment, container prisoners' details.
- 2013 - A University Health Board was fined when a bag containing personal details fell off a Psychiatrist's bicycle.
- 2013 - A Council was fined £80,000 for losing an un-encrypted memory stick containing details of children in its care. The memory stick was taken from a laptop in the Council's offices and was never found.
- 2013 - A Payday Lender was fined £175,000 for sending unsolicited text messages.
- Several Government departments have also famously mislaid laptops!

Compromises to data security are usually as a result of human error.

HOW TO AVOID BEING COMPROMISED BY STAFF CLICKING ON LINKS IN PHISHING EMAILS

- Ensure software is up-to-date
- Install security software
- Enforce Policies and Procedures
- Educate staff

KEY DEFINITIONS

DATA SUBJECTS:

May include individual customers and also employees.

CONTROLLERS:

Organisations or individuals who process data for legitimate purposes. An organisation is normally the DATA CONTROLLER, rather than an individual employee.

DATA PROCESSOR:

An organisation or an individual who processes data on behalf of a Controller / organisation - eg: an outsourced service provider. The GDPR does not consider employees of the Controller / organisation, to be Processors.

PROCESSING:

An activity relating to personal data, from initial collection through organising, altering, consulting, using, disclosing or combining, to the final destruction. This includes holding data, either electronically or manually.

SEVEN KEY PRINCIPLES

1. FAIR, LAWFUL AND TRANSPARENT PROCESSING.

Processing data fairly and lawfully. This includes an obligation to tell the individual what his/her data will be used for.

Example: Carrying out a contract with a person, but then the contact details may be used or passed on for marketing purposes. THIS WILL NOT BE ALLOWED UNDER THE GDPR unless the person has given specific consent and the exact nature of the further processing is disclosed and agreed to.

2. THE PURPOSE OF LIMITATION PRINCIPLE

Using information only for the specified, explicit and legitimate purposes for which the data was collected and not for any other purpose.

Some archiving and statistical purposes are still allowed. DATA COLLECTED FOR ONE PURPOSE MAY NOT BE USED FOR ANOTHER PURPOSE.

3. DATA MINIMISATION

Only the personal data actually needed to achieve the intended purpose, may be collected. Personal data should be adequate, relevant and limited to what is necessary and such data must be kept up-to-date.

Every reasonable step must be taken to erase or correct inaccurate data.

Organisations cannot collect data on a 'just in case it becomes useful' basis. THINK CAREFULLY ABOUT WHAT PERSONAL DATA IS WANTED FOR.

Obtain informed consent from individuals for anything the organisation might subsequently wish to do with the data collected.

4. ACCURACY

Data Collectors are responsible for taking reasonable steps to ensure that personal data is accurate.

5. DATA RETENTION PERIODS

Data must not be kept for longer than necessary, and the 'right to be forgotten' must always be considered.

6. DATA SECURITY

Controllers / organisations are responsible for the data collected. This includes the security of the data when it is being processed by a third party, as well as by the Controller/ organisation itself.

Security refers to external and internal threats. For example: hackers and badly trained internal staff.

Security of both electronic and paper records is required.

7. ACCOUNTABILITY

The Controller / organisation is responsible for compliance with the data protection principles and must be able to demonstrate the steps taken to ensure compliance.

WHAT TO DO TO ACTIVELY COMPLY WITH THE GDPR

Obtain consent from the individual. Consent is the usual lawful basis for obtaining and processing personal data. The processing of sensitive personal data is only permitted under certain conditions:

- Explicit consent
- Employment law
- Vital interests
- By charitable or not-for-profit bodies
- Data manifestly made public by the individual
- Legal claims
- Reasons for substantial public interest
- Medical diagnosis and treatment
- Public health
- Historical, statistic or scientific purposes
- Exemptions under National Law

When performing a contract, such as the delivery of a service, lawful purpose covers the following:

- Processing address details for the delivery of goods.
- Taking payment for purchases.
- Responding to enquiries during pre-contractual relations.

OBTAINING CONSENT

Individuals must be provided with a CLEAR EXPLANATION of the data processing to which they are consenting. There must be a CLEAR OPT-IN to this consent and it must be entirely voluntary and freely given.

It is unacceptable to rely on inaction, opt-out, pre-checked fields or silence.

Consent must always be obtained from the individual and not from a third party (other than where there is authorisation, such as a Power of Attorney.

The individual must signify consent by clear, affirmative action and organisations need to demonstrate that this has been given.

There must be no element of compulsion or undue pressure. This will invalidate consent.

There cannot be blanket, open-ended or catch-all consent wordings. The consent must be explained clearly, intelligibly and precisely, covering the scope and purpose of the data processing and the context.

This information must be given in clear language, WITHOUT JARGON. The Controller must be identified, as well as the purposes for which the data will be processed.

INFORMATION TO PROVIDE TO AN INDIVIDUAL:

- The Controller's identity and location
- The purpose of processing
- Any third-party involvements
- Access and correction rights
- The right 'to be forgotten' and to object
- The right to withdraw consent
- The mechanism for exercising rights

WAYS TO OBTAIN CONSENT

One of the biggest changes under the GDPR is the requirement to obtain consent from individuals.

ONLINE

- Ticking a box
- Choosing settings
- Downloading instructions

OFFLINE

- Signing a Data Protection Authorisation
- Completing a form

UNACCEPTABLE METHODS

- Silence
- Pre-ticked options
- Failure to opt-out
- Any passive reaction

The consent must be separated and distinguishable from other matters. This means that it cannot be buried amongst other terms and conditions. It can be in the same document, but it must be CLEARLY DISTINGUISHABLE.

WITHDRAWING CONSENT

This is not a 'retrospective' right, so consent cannot be withdrawn for processing that has already occurred.

Organisations should consider the mechanism for this to happen and put a process in place. This process must be told to the individual.

PRE-EXISTING CONSENT UNDER PREVIOUS LAW

Any pre-existing consent under previous law, that does not fulfil the requirements of the GDPR, NEEDS TO BE RE-APPLIED FOR.

This is likely to concern marketing organisations.

INDIVIDUAL'S RIGHTS UNDER THE GDPR

Individuals have the rights to:

- Transparent, clear and concise information
- Access to personal data
- Rectification
- Be forgotten
- Restrict processing.
- Data portability
- Not be evaluated on the basis of automated processing
- Object to processing
- Be informed of their rights

Communication must be transparent, clear and sufficient, but it must not be overwhelmingly long. Privacy Policies should be easy-to-read and to understand.

RIGHT TO REVIEW INFORMATION

Individuals have a legal right to review information held about them.

Controllers are allowed to request 'proof of identity' before giving out information - but this is not obligatory. If the Controller cannot link the data to an individual, then the Controller is not forced to take steps to identify that individual and can simply refuse the request.

There is a time limit of ONE MONTH for supplying requested data. In special circumstances, this could be extended to a maximum of three months.

ACCESS RIGHTS

- Confirmation of how and where their personal data is being processed
- Information about the purposes of processing
- Information about the categories of data being processed
- Information about the categories of recipients with whom data is being shared
- Information about the period of time the data will be stored and the criteria for determining this
- Details of their rights in terms of erasure, rectification, restriction of processing to make objections
- Details of their right to complain to the ICO
- The source of the data
- Information about the logic of automated processing
- Obtaining a copy of the individual personal data held

CHARGES

Controllers are permitted to charge a REASONABLE FEE for the provision of information, where the request is repetitive, manifestly unfounded or excessive for further copies. Otherwise there should be no charge.

Inaccurate or incomplete data must also be rectified or erased.

THE RIGHT 'TO BE FORGOTTEN'

Deletion of all personal data (the 'right to be forgotten') may be requested by the individual if the continued processing is unjustified. This can only be determined when the retention of data is not compliant with the GDPR.

Circumstances where the ‘right to be forgotten’ applies:

- The data is no longer needed.
- The processing was based on consent that it is withdrawn.
- Objection by the individual.
- Unlawful processing.
- Compliance with the law.

There may be occasions when grounds for continued processing would override an objection.

RESTRICTING PROCESSING MIGHT APPLY IF:

Accuracy is contested.

- There is unlawful processing
- Data is required for legal cases
- There is a pending request for erasure

The Controller must ensure that the request is actioned by any third parties involved in the processing of the data.

It is important that organisations identify these third parties.

Individuals also have the right to:

Data Portability:

Data to be provided in a format that can be transferred easily - PDFs, for instance.

Direct Marketing:

It is important to ensure that there is an easy process for unsubscribing.

(DATA) CONTROLLERS and (DATA) PROCESSORS

Controllers are accountable for compliance with the GDPR and are responsible for all the processing that occurs with the data collected.

Processors also have direct compliance obligations and can face direct enforcement actions or penalties.

CONTROLLERS

Nearly all organisations are Controllers - even if the data held is about its own employees.

The Controller is defined as the entity that determines the use to which personal data is put … why and how it is processed.

In cases where they may be 'Joint Controllers', arrangements for collaboration must be put into place. Normally, this would be dealt with in the Terms and Conditions between the parties, and such agreements should cover the data protection responsibilities of each party.

Joint Controllers are equally liable for any breaches for failures.

Controllers must be able to demonstrate that they are compliant with the GDPR, and they are accountable for the actions of all Processors used.

Controllers should also maintain Policies and Procedures about all the Processors involved, including the checking and updating of contractual agreements with third parties, the monitoring of third party Privacy Policies and security.

Organisations whose core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale, must:

- Appoint a dedicated Data Processing Officer
- Keep records of processing activities
- Ensure that processing information is available to the ICO.

DATA SECURITY

Keeping data secure is in the interests of organisations, as well as a requirement of GDPR.

Appropriate measures should be taken against unauthorised or unlawful processing or disclosure of personal data, and against accidental loss, destruction of or damage to personal data.

These include:

- Encryption
- Ongoing security reviews
- Back-up and restore facilities
- Regular testing of contingency plans and security

Areas where consideration should be given

- Smartphone security, password protection and erasing, if lost
- Laptop encryption and the amount of data held
- Physical security of filing and office computers
- Password protection and resetting
- Internet security and spyware protection
- Email encryption, secure messaging and secure file sharing
- Information held online via third party servers
- Back-up drives
- Secure document disposal
- Visibility of computer screens
- Telephone conversations in public, or insecure environments
- 'Bring your own device' policies on employee's personal equipment

The organisation must consider the risks of data falling into the wrong hands and outline the steps to be taken to minimise or prevent these risks.

REPORTING A BREACH

There is an obligation to report any data security breaches to the ICO without delay within 72 hours. The individual whose data may be breached, must also be notified of the breach, in order to protect themselves.

The only exception to this reporting requirement is when the data breach is unlikely to result in harm to the individual.

Records of all breaches must be kept.

Notification to the ICO must include:

- A description of the breach, including numbers and categories
- A contact name and details
- An assessment of the likely consequences
- The measure taken to mitigate or remedy the situation

PROCESSORS

A Processor is any organisation or individual processing data on the Controller's behalf. This does not include the employees of the Processor.

Controllers must only appoint Processors who comply with the GDPR and can guarantee that this is so.

Processors also have direct compliance obligations under the GDPR and can face direct enforcement actions or penalties.

There must be a written, binding agreement in place that includes:

- Only acting on the Controller's instructions
- Confidentiality obligations for all personnel with access
- Data security obligations
- Returning or destroying data at the end of a relationship

If a Processor starts deviating from the Controller's instructions, it will be Controller who is responsible under the GDPR.

The Processor must also comply with requirements for:

- Record keeping
- Security
- Breach reporting
- Data Protection Office appointment

Processors may also be liable for breaches.