GDPR: AN INTRODUCTION

HELPING ORGANISATIONS NAVIGATE A SAFE AND SUCCESSFUL PATH TO GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

CONTENTS

GDPR - AN EXECUTIVE SUMMARY

The new General Data Protection Regulation (GDPR) is the most significant development in the area of data privacy for the past 20 years and it will affect organisations globally. GDPR concerns the protection of personal data of, or relating to EU citizens. This identification can be either direct or indirect. Since it is applicable to EU citizens on the whole, it is non EU border specific – this means that it will also apply to organisations outside Europe i.e. wherever it may be stored and/or processed.

Given the broad territorial application of the GDPR, businesses have until 25th May, 2018, to consider and implement the necessary provisions to meet this new regulation or face a potential fine of up to €20 million or 4% of annual global turnover, whichever is higher, for any personal data breaches as a result of non-compliance.

It is important to mention that even though the UK is in the midst of Brexit, it is highly likely that some, or even all, of the GDPR's provisions may be transposed into UK law. Although the specifics are obviously not yet known, it is likely that this may occur via an amendment to the Data Protection Act 1998 (DPA) or by repeal and enactment of new UK legislation.

Over and above the initial awareness required and the definition of an approach to tackle this issue, part of the solution required may be to implement a document/content management system. Encryption, including PC, server, network and printer hard drive encryption, are also likely to minimise the impact in case of a data breach. Such tools will bring automated benefits in terms of personal data processing i.e. identification, classification, monitoring, tracking and more importantly, the deletion retention timescales required to meet GDPR timelines and guidelines.

If not already done, organisations should not delay and start immediately with the audit of their existing data practices, policies and equipment and put in place timelines for implementation of the new changes required to meet GDPR guidelines and timescales.

The European Commission will work closely with Member States Data Protection Authorities (see recital 20 [1*]), in the case of the UK – the Information Commissioners Office (ICO), to ensure a uniform application of the new rules and will work to inform citizens about their rights and companies about their obligations.

[1*] recital 20 states - "20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;". (Source: GDPR)

INTRODUCTION TO UK AND EU DATA PROTECTION

The (UK) Data Protection Act 1998 (DPA)

The **Data Protection Act 1998 (DPA)** is a United Kingdom, act of Parliament, which defines the law on the processing of data on identifiable living people. It is the main piece of legislation that governs the data protection in the UK. This well-known piece of legislation controls how your personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. In general, they must make sure the information is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure; and
- not transferred outside the European Economic Area (EEA) without adequate protection.

The DPA (1998) replaced and consolidated earlier legislation; such as the **Data Protection Act 1984** and the **Access to Personal Files Act 1987.**

The EU Data Protection Directive (officially Directive 95/46/EC)

In 1998, The Data Protection Act 1998 (DPA) was enacted to bring British law into line with the 1995 EU Data Protection Directive (officially **Directive 95/46/EC**). The main focus was to bring the protection of individuals (i.e. processing of personal data), in line with EU freedom of movement of people and goods. In practice it provided a way for individuals to control information about themselves and so **seven principles** governing Directive 95/46/EC were introduced. These were:

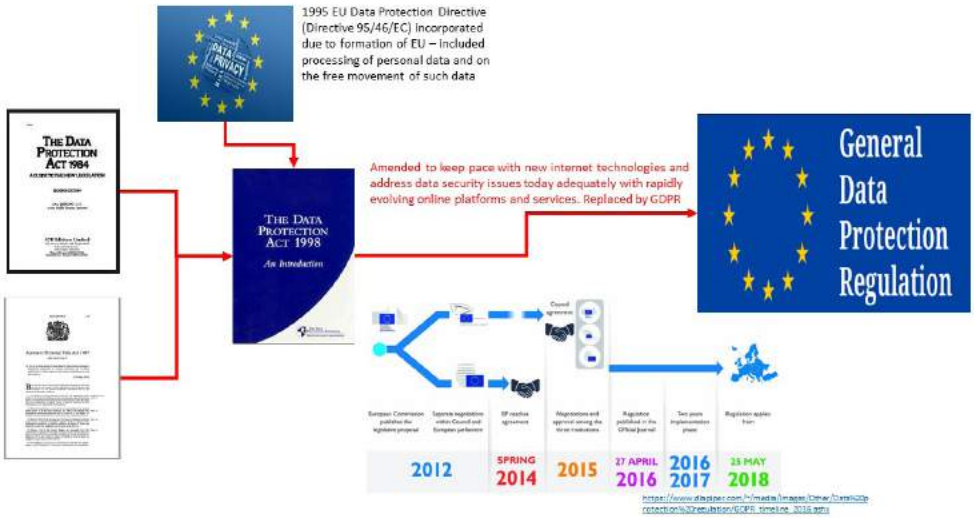
- Notice—data subjects should be given notice when their data is being collected;
- Purpose—data should only be used for the purpose stated and not for any other purposes;
- Consent—data should not be disclosed without the data subject's consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—data subjects should be informed as to who is collecting their data;
- Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

As a directive the member states, within the limits of the provisions, determine more precisely the conditions under which the processing of the personal data is lawful. Therefore various interpretations of the directive were present throughout the EU member states.

The Data Protection Regulation (GDPR) (officially Regulation (EU) 2016/679)

Adopted in April 2016, the General Data Protection Regulation (GDPR - officially EU data **protection regulation (EU) 2016/679** of the European parliament) will supersede previous Data Protection Directives (including the UK's Data Protection Act 1998 (DPA)) without the need for further national legislation. GDPR will be enforceable, throughout Europe, starting on the **25th May, 2018.**

The diagram below illustrates the Data Protection Legislation over the years.



*Source: KYOCERA

The primary objective of the GDPR is to give citizens back more control of their personal data. It will strengthen and unify data protection for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU. If an organisation suffers a data breach, under the new EU compliance standard, the following may apply depending on the severity of the breach:

- An organisation must notify the local data protection authority and potentially the owners of the breached records;
- An organisation could be fined up to 4% of global turnover or €20 million.

However, GDPR does provide exceptions based on whether the appropriate security controls are deployed within the organisations. For example: a breached organisation that has rendered the data unintelligible through encryption, to any person who is not authorised to access the data, is not mandated to notify the affected record owners. This is an important point to bear in mind, and although it is not an all-inclusive point, it will go a long way to assisting with compliance of GDPR and potentially avoiding a fine.

The chances of being fined are also reduced if the organisation is able to demonstrate a "secure breach" has taken place.

To address the GDPR compliance requirements, organisations may need to employ one or more different encryption methods within both on-premise and cloud environments, including the following:

- Servers, including via file, application, database, and full disk virtual machine encryption;
- PC and peripheral hard drives, including those found in printers, through encryption;
- Storage, including through network-attached storage and storage area network encryption; and
- Networks, for example through high-speed network encryption e.g. VPNs.

GDPR - A COMPLIANCE/ REGULATORY OVERVIEW

The original European Data Protection Directive framework (Directive 95/46/EC) had been in existence since October 1995. Advances in IT, such as the internet, social media sites, online banking, cloud based services/solutions etc., have highlighted some short comings in this old directive. As a result, on the 27 April 2016, the new EU data protection regulation (EU) 2016/679 of the European parliament has effectively replaced the old directive. This is more commonly known as the General Data Protection Regulation (GDPR), and has at its main objective to ease the flow and regulation concerning personal data across the 28 EU member states.

This section of the document summarises the main impacts and changes as a result of the GDPR directive (for a copy of this see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

This section of the document will also provide more information regarding tools and technology i.e. document management and associated systems/solutions, encryption and their relation and inter-relation with GDPR.

The key GDPR features and changes to the European Data Protection Directive are as follows:

- Regulation vs. Directive: the new EU data protection regulation - (EU) 2016/679 of the European parliament/General Data Protection Regulation (GDPR) is a regulation. This means that the same regulation is passed and is applicable across all 28 EU member states i.e. there are no local "clones/interpretations" per EU state (as would happen in a directive).
- Significantly increased fines: Companies can be fined up to €20 million or 4% of annual global turnover for breaches of data protection law. The level of fine imposed will depend on the seriousness or repeated nature of a breach. This will be determined by a local country's supervisory authority.
- Over and above the fines, enterprises may also be subject to:
  - Mandatory audits rights from the appropriate Data Protection Authorities (DPAs); and
  - Enforcement notices. Further information on these will be available in due course from the Information Commissioners Office (ICO).

As an early example of indicative fines:

1) Hampshire County Council – In August 2016, Hampshire County Council was hit with a £100,000 fine by the Information Commissioner's Office (ICO) after documents containing personal details of over 100 people were found in a disused building. Files were found containing Social Care cases and complaints. The documents contained confidential information and sensitive (personal) data. It also found 45 bags of confidential waste in another locked room. The ICO has the power to impose a monetary penalty on a data controller of up to £500,000.

2) A Northern Ireland NHS Trust – In 2010, a NHS Trust in Northern Ireland was fined £225,000 by the ICO, following unauthorised access by trespassers to medical and staff records held in a disused building. Records on site included 100,000 medical records, and 15,000 staff records, including unopened wage slips. The records were found stored in boxes, in cabinets, on shelves or on the floor.

3) Scottish Borders Council – In September 2012, Scottish Borders Council was fined £250,000 by the ICO after former employee details were found in a paper recycle bank. The records included former employees' pension details and salary and bank account data. A third party was contracted to digitise the records but failed to seek appropriate guarantees on how the personal data would be kept secure. The files were spotted by a member of the public who called police, prompting the recovery of 676 files. A further 172 files deposited on the same day, but at a different paper recycling bank, are thought to have been destroyed in the recycling process.

- Individuals rights are strengthened: under GDPR for example unambiguous consent to use private data, the right to-be-forgotten and the right to data portability:

    - Enhanced definition of consent: The European Parliament's press release highlights the GDPR's provisions on clear and affirmative consent to the processing of private data by the person concerned, so as to give consumers more control over their private data. This could, for example, mean ticking a box when visiting an internet website or by another statement or action clearly indicating acceptance of the proposed processing of the personal data. Silence, pre-ticked boxes, or inactivity will thus not constitute consent. It should also be as easy for a consumer to withdraw consent as to give it. The new GDPR also puts an end to "small print" privacy policies and information now should be given in clear language before the data is collected.

    - The Right-To-Be-Forgotten (Recital: 66): states 'To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.'

    - The right to Data Portability: Individuals are/will be entitled to easier mechanisms for the transfer of their personal data between service providers even though concerns have been raised as to the administrative burden that this may place on data controllers. Article 20 of GDPR states:

        - 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

            - (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
              (b) the processing is carried out by automated means.

        - 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

TalkTalk

1) Telecoms company TalkTalk has been issued with a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data "with ease". The ICO's in-depth investigation found that an attack on the company last October could have been prevented if TalkTalk had taken basic steps to protect customers' information. ICO investigators found that the cyber attack between 15 and 21 October 2015 took advantage of technical weaknesses in TalkTalk's systems. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes. However, "despite criticism from some quarters that it got off lightly and that under the new EU data laws (GDPR) it could have faced a £ m penalty [1]".

[1] http://www.decisionmarketing.co.uk/news/talktalk-could-have-faced-70m-fine-under-gdpr

- 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

- Expanded compliance: Controllers and processors must demonstrate compliance of GDPR by adopting detailed processing of records. Direct accountability on processors and controllers of information. Under the old regulation, there was no obligations posted on processors (i.e. service providers) of data/information. Under GDPR, processors are directly accountable for data protection rules. This has a particular impact on Cloud providers, for example, that provide services containing EU residents' data. The effects of the above can be mitigated by implementing a Content Management (CM) system. For example, details of who the processor is? Controller is? Data subjects involved in controlling? Categories of data? Sensitive data? Etc. are required to meet expanded compliance requirements.

- Direct and indirect identifiers: In contrast to the old directive, GDPR puts beyond any reasonable doubt the criteria used in identifying persons and specifically includes 'location data' and 'an online identifier' (e.g. Unique Identifiers (UIDs)) criteria (see 'personal data' definition – Glossary of terms).

- Mandatory breach reporting: The GDPR imposes a requirement on data controllers to notify data breaches without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. This must be reported to the national data protection authority (the ICO in the case of the UK) 'In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.' You are exempt if the information is unlikely to cause personal harm or is high risk to the individual. Encrypted data will be exempt from reporting.

- Establishment outside the EU/extra-territoriality: The directive will apply to all organisations, irrespective of a presence in the EU – i.e. if an organisation trades/offer goods and services with the EU, then it needs to comply with GDPR. The law therefore is applicable if you are established within the EU; or offer services to EU residents; or monitor the behaviour of EU residents.

- Brexit is no excuse: As previously mentioned; even though the UK is in the midst of Brexit, it is highly likely that some, or even all, of the GDPR's provisions may be transposed into UK law. Although the specifics are obviously not yet known, it is likely that this may occur via an amendment to the Data Protection Act 1998 (DPA) or by repeal and enactment of new UK legislation.

- Data Protection Officers: Entities will be obliged to appoint a Data Protection Officer (DPO) where, on a large scale and as part of their core activities, they regularly and systematically monitor data subjects or process sensitive personal data. SMEs (i.e. enterprise less than 250 employees) will be exempt where data processing is not their core business activity. An organisation employing fewer than 250 people is exempt from keeping records (unless it processes personal data classified as high risk).

The 3 main criteria under which you must appoint a DPO is (Article 35) if your core activity is in:

- 'large scale' systematic monitoring of individuals;
- 'large scale' processing of sensitive data; or
- public authorities.

For reference, the exact mandate (Article 35) words are:

"(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale."

A DPO can either be a part-time role or combined with other duties. In performing the role, the DPO must however have an independent reporting line (like most compliance officers), be empowered and report directly to the board without interference.

Other important GDPR changes include:

- Data access requests: The statutory fee of €6.35 for an access request will be abolished however, organisations will welcome a new provision where requests are received that are manifestly unfounded or excessive, in which case the controller may charge a reasonable fee or may refuse to act on the request. i.e. - a country's supervisory authority will now likely raise money through fines rather than the statutory data access request fee(s).

- One stop shop: The initial commission proposal of a one stop shop mechanism was expected to be watered down considerably and the current state of play is that multinationals who have multiple establishments across Europe will deal with the supervisory authority of the Member State in which the company has its "main establishment." There are circumstances, however, in which the lead supervisory authority will be required to consult and co-operate with authorities within other affected Member States.

- Privacy Impact Assessments (article 35 of GDPR is the fact that data protection impact assessments (DPIA) are mandatory for organisations with technologies and processes that are likely to result in a high risk to the rights of the data subjects. Ref: http://www.itgovernance.co.uk/blog/gdpr-and-privacy-impact-assessments-why-are-they- required/).

- Effective date: the GDPR comes into force on the 25th May 2018. All organisations that process the personally identifiable information(PII) of EU residents will be required to abide by a number of provisions or face significant fines.

See more information at:

GDPR REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

GDPR AND TECHNOLOGY

PRINTERS

Today's office print devices have come a long way from the standalone basic devices that once existed. Nowadays, printers and multi-function products (MFPs) are intelligent networked assets, that like a PC, contain a screen, a keyboard, a hard drive (which can potentially store sensitive information), and an Operating System (OS).

Increased cybercriminal activity that is directly targeted at networked devices, including printers, has been highlighted as a weak link in the defence against corporate data theft and malicious attack. Printers have known vulnerabilities that if exploited, can allow attackers to breach a business' network.

Most enterprises actually overlook printer security and therefore these could be infected by malware that end up compromising the entire network. To complicate the matter, regulatory changes such as GDPR, that contain potential ruinous financial and legal implications for non-compliance. Organisations must take immediate action to incorporate MFDs into their overall data protection strategy.

GDPR references that there are two main technological areas that need to be considered when addressing compliance of personal data, these are:

1) Data Management – i.e. the collection, retention and destruction of data (i.e. the end-to-end of Data Management; and

2) Data Security/Encryption – i.e. the processing and handling of data, which involves encryption of the data as a technology. Unfortunately, GDPR does not provide much exact guidance in terms of which technology (see recitals 66, 67, 68, 71, 78, 81, 156, 168) and/or security (see article 32) to use, instead citing only that the "appropriate" and "state of the art technical protection measures" be implemented. This may be vague on purpose, as technology "evolves", so too the technology deployed should "evolve". This may ultimately have to be debated in a court of law, as to what is "state of the art" at the time of a potential breach.

Although vagueness in this area makes interpretation of the regulation difficult, at Annodata we believe that the implementation of a technical solution(s) will make compliance with GDPR, easier and more efficient when compared to manual processing. It is also probably the most cost effective option to progress, taking into consideration the following GDPR requirements:

- data accuracy (see article 5 – up to date data),
- immediate access (see article 15 - a company's ability to satisfy a Subject Access Request), and
- data retention and erasure (also referred to as the right-to- be-forgotten (RTBF) (see articles 16 and 17).

Many companies will not know how to approach and start classifying data, which may incidentally be stored across many IT systems. There are many automated data classification and processing technologies are now available on the market, including those available from Annodata, that can be used as a solution in this area.

Data encryption is an important data protection technology called out in GDPR and again article 32 suggests the "pseudonymisation and encryption of data; ability to ensure confidentiality, integrity, availability and resilience of processing; the ability to restore data after an incident; and a process for testing, assessing and evaluating effectiveness of security".

The bottom line is can you, as an organisation, and in a court of law defend the actions and processes that you took to implement GDPR; thereby limiting a company's liability of a fine i.e. has your organisation been able to assess the relevant data protection liabilities and make a judgement accordingly?

GDPR TOP 5 MYTHS DISPELLED

MYTH #1 - UNDER BREXIT, UK BUSINESSES ARE NOT REQUIRED TO CONFORM TO GDPR

(1*)It is important to mention that even though the UK is in the midst of Brexit, it is highly likely that some, or even all, of the GDPR's provisions may be transposed into UK law. Although the specifics are obviously not yet known, it is likely that this may occur via an amendment to the Data Protection Act 1998 (DPA) or by repeal and enactment of new UK legislation.

MYTH #2 - I HAVE TO APPOINT AN INDEPENDENT AND QUALIFIED DATA PROTECTION OFFICER (DPO)

The 3 main criteria under which you must appoint a DPO is (Article 35) is if an organisation is dealing with:

- 'large scale' systematic monitoring of individuals;
- 'large scale' processing of sensitive data; or
- Is a public authority.

The DPO does not have to be a full-time employee of the organisation. This function can be outsourced, if required. If an/your organisation does not fall under the above criteria, it means that they do not have to appoint an external person. In fact, this can be an employee, and it can be either a part-time role or combined with other duties, but in performing the role, the DPO must have an independent reporting line (like most compliance officers), be empowered and report directly to the Board without interference. What is important, is that the appointed person must be a data protection professional with 'expert' knowledge of data protection law and practices to perform their duties and ensure your organisation achieves and maintains compliance. The person appointed should ideally implement a strategy and project, with the key objective of meeting/exceeding the GDPR compliance. The project must implement organisational, procedural and technical measures to demonstrate compliance.

MYTH #3 - I DO NOT HAVE ANYTHING TO DO WITH STORING MY DATA, THEREFORE I AM NOT LIABLE UNDER GDPR

Under GDPR, both controllers and processors are equally liable and must demonstrate compliance of GDPR by adopting detailed processing of records. Under the old regulation, there was no obligations posted on processors (i.e. service providers) of data/ information. However, under GDPR, processors are directly accountable for data protection rules. This has a particular impact on Cloud providers, for example, that provide services containing EU residents' data. The effects of the above can be mitigated by implementing an enterprise content management system (ECM), using an appropriate document management system. For example, details of who the processor is? Controller is? Data subjects involved in controlling? Categories of data? Sensitive data? Etc.

Companies should use GDPR as a cornerstone for a risk mitigation process. There is no longer a limitation of liability, as now both the controller and subcontracted processors are equally liable for a data breach (see Articles 24, 26, 27, 28 and 29).

1*source https://www.linkedin.com/pulse/why-brexit-happen-data-protection-eduardo-ustaran?articleId=6062985867032983824#comments-6062985867032983824&trk=sushi_topic_posts

MYTH #4 - I HAVE IMPLEMENTED A DOCUMENT MANAGEMENT / CONTENT MANAGEMENT SYSTEM, THEREFORE I AM GDPR COMPLIANT.

Unfortunately, GDPR does not provide much exact guidance in terms of which technology and/or security to use, instead citing only that the "appropriate" and "state of the art technical protection measures" be implemented. This may be vague on purpose, as technology "evolves", so too the technology deployed should "evolve". This may ultimately have to be debated in a court of law, as to what is "state of the art" at the time of a potential breach.

Although vagueness in this area makes interpretation of the regulation difficult, at Annodata it makes logical sense to say that the implementation of a technical solution, such as a content management system, will make compliance with GDPR, easier and more efficient when compared to manual processing. But without the correct processes and focus on what GDPR refers to as "the embodiment of the concept of privacy by design", just having a content management system, does not imply compliance with GDPR.

MYTH #5 – I HAVE ALL MY SYSTEMS ENCRYPTED, THEREFORE, I AM GDPR COMPLIANT

In terms of fines imposed, GDPR does provide an important exception based on whether the appropriate security controls are deployed within the organisation. For example: a breached organisation that has rendered the data unintelligible through encryption to any person who is not authorised to access the data, then the organisation is not mandated to notify the affected record owners. This is an important point to bear in mind, and although not all-encompassing, it will go a long way to assisting with compliance of GDPR and mitigating the risk of being fined.

GLOSSARY OF TERMS

Consent - freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten (RTBF), it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority – A national authority tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union. For purposes of the UK, this authority will be the Information Commissioners Office (ICO) -https://ico.org.uk/

Data Protection Officer (DPO) - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject - a natural person whose personal data is processed by a controller or processor

Directive - a legislative act that sets out a goal that all EU countries must achieve through their own national laws

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Enterprise / Organisation - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

GDPR - The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). GDPR concerns the protection of personal data of, or relating to EU citizens

Personal data - is "any information relating to an identified or identifiable natural person". Identification can be direct or indirect, and includes such identifiers as "a name, identification number, location data, online identity, one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that person" (see Article 4 [1]). Profiling is also included, and this would include "assessing a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (see GDPR, Article 4 [4]). For purposes of this document - Personal data may also be referred to as Personally Identifiable Information or PII (see below)

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Personally Identifiable Information (PII) - Is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Pseudonymisation of data - Is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. (Source – Wikipedia)

Recipient - entity to which the personal data are disclosed

Regulation - a binding legislative act that must be applied in its entirety across the European Union

Representative - any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities

Right to be Forgotten (RTBF) - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority - a public authority which is established by a member state in accordance with Article 46

(Source - EU GDPR Glossary, unless otherwise specified e.g. Wikipedia)

Annodata is one of the UK's longest standing, independent and fastest growing providers of ICT and document management services.

For more information on how Annodata can help you become a more efficient enterprise, please contact:
marketing@annodata.co.uk
or Tel: 01923 333 333

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY