GDPR Training

The 2414 Group

- Previously known as ARC NetSec
- Started as IT Services back in 2004
- 2414Red – Networking & Cyber Security
- 2414Blue – Training and Education Svs
- 2414Green – Digital Marketing and Advertising

Industry Facts

- 80% of breaches are as a result of human error
- 60% of breaches were linked to a 3rd party
- 75% of companies in the UK suffered an attack or breach of some description
- 60% of organisations don't have a security budget

***Data taken from various technology vendors and Gartner

Our Customers Include

Module 1

GDPR introduction, definitions and penalties

The nature of European Law

Two main types of legislation:

Directives
Require individual implementation in each Member State
Implemented by the creation of national laws approved by the parliaments of each Member State
European Directive 95/46/EC is a Directive
UK Data Protection Act 1998

Regulations
Immediately applicable in each Member State
Require no local implementing legislation
EU GDPR is a Regulation

Article 1 : Subject-matter and objectives

Natural person = a living individual

Natural persons have rights associated with:
The protection of personal data
The protection of the processing personal data
The unrestricted movement of personal data within the EU

Article 2 : Material scope

- In material scope:

Personal data that is processed wholly or partly by automated means;
Personal data that is part of a filing system, or intended to be.

- Out of material scope:

Personal data that is used in course of an activity outside of EU Law;
Personal data such as border checks, asylum and immigration status;
Personal data that is used in relation to a purely personal activity;
Personal data used for the purpose of crime prevention, etc.

- Territorial Scope, it relates to where the data is processed not where your office is located

Remedies, liability and penalties

Article 77: Right to lodge a complaint with a supervisory authority

- Every data subject has the right to launch a complaint with a supervisory authority
- In Member State of habitual residence
- Place of work
- Place of alleged infringement

- Supervisory authority shall inform the complainant of progress, including the possibility of judicial remedy

Remedies, liability and penalties cont'd…

Article 78: Right to an effective judicial remedy against a supervisory authority

- Right to judicial remedy against a legally binding decision.
- Right to judicial remedy where the supervisory authority does not handle a complaint or does not inform data subject of progress or outcome.
- Judicial remedy shall be brought before the courts of the Member State where the supervisory authority is established.
- Supervisory authority must provide opinion or decision of the Board to the court.

Remedies, liability and penalties cont'd…

Article 79: Right to an effective judicial remedy against a controller or processor

- Right to judicial remedy where their rights have been infringed as a result of the processing of personal data.
- Proceedings shall be brought before the courts of the Member State where the controller or processor has an establishment.
- Proceedings may be brought before the courts of the Member State where the data subject habitually resides.

Remedies, liability and penalties cont'd…

Article 82: Right to compensation and liability

- Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor. Controller involved in processing shall be liable for damage caused by processing.
- Processor liable only for damage caused by processing or where it has acted contrary to lawful instructions of the controller.
- Exemption for controller and processor where they are not responsible. Joint and several liability to ensure effective compensation.
- Compensation clawback provision.

Remedies, liability and penalties cont'd…

Article 83: General conditions for imposing administrative fines

- Imposition of administrative fines will in each case be effective, proportionate, and dissuasive.

- Administrative fine imposed in addition to, or instead of, the corrective powers of the supervisory authority in Article 58(2):

- Issue warnings;
- Issue reprimands;
- Order compliance with Data Subjects requests;
- Communicate the Personal Data breach directly to the Data Subject

The Fines… 2%

€ 10,000,000 or, in case of an undertaking, 2% total worldwide annual turnover in the preceding financial year (whichever is greater):
8: Child's consent
11: Processing not requiring identification
25: Data protection by design and by default
26: Joint controllers
27: Representatives of controllers not established in EU
26 -29 & 30: Processing
31: Cooperation with the supervisory authority
32: Data Security
33: Notification of breaches to supervisory authority
34: Communication of breaches to data subjects
35: Data protection impact assessment
36: Prior consultation
37 -39: DPOs
41(4): Monitoring approved codes of conduct
42: Certification
43: Certification bodies

TWO FOUR ONE FOUR

Module 2

Principles

Principles – Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

***The most important element with the above is accountability

Article 5: Principles relating to the processing of personal data

- The principles largely remain the same:
- Processed fairly and lawfully.
- Collected for specified, explicit and legitimate purposes. Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Processed in a manner that ensures appropriate security.

- Introduction of the new requirement that the controller be able to demonstrate accountability

Article 9: Processing of special categories of personal data

- Processing of following types of personal data are prohibited: Race
- Ethnic origin
- Political opinions
- Religion
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Concerning a natural person's sex life
- Sexual orientation.

Article 9: Processing of special categories of personal data

Exceptions:

- The data subject has given explicit consent;
- It is necessary to fulfil the obligations of controller and data subject;
- It is necessary to protect the vital interests of the data subject;
- Processing is carried out by a foundation or not-for-profit organisation;
- The personal data has been made public by the data subject;
- Establishment, exercise or defence of legal claims;
- Reasons of public interest in the area of public health; Archiving purposes in the public interest;
- A Member State has varied the definition of a special category.

Module 3

Rights of Individuals - PII

Section 1: Transparency and modalities

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

The controller shall provide any information or communication referring to the data subject in a

- concise,
- transparent
- intelligible and
- easily accessible form;
- using clear and plain language;
- in particular for any information addressed specifically to a child.

Time period reduced from 40 days to 30 days

Fees abolished

Section 2: Information and access to personal data

Article 13.1: Information to be provided where personal data collected from the data subject

When obtaining personal data, the controller shall provide the data subject with all of the following information:

- the identity and contact details of the controller and their representative;
- the contact details of the data protection officer;
- the purposes of the processing of as well as the legal basis for the processing; the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- the fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

Section 2: Information and access to personal data

Article 13.2: When obtaining personal data the controller shall provide the data subject with the following further information to ensure fair and transparent processing:

- the period of time that the data will be stored;
- the right to rectification, erasure, restriction, objection;
- the right to data portability;
- the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- the consequences of the data subject failure to provide data;
- the existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject.

Section 2: Information and access to personal data

Article 14: Information to be provided where the personal data have not been obtained from the data subject

Where personal data has not been obtained directly from the data subject:
the identity and contact details of the controller and their representative;

- the contact details of the data protection officer, where applicable;
- the purposes as well as the legal basis of the processing;
- the categories of personal data concerned;
- the recipients of the personal data, where applicable;
- the fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

Section 2: Information and access to personal data

Article 15: Right of access by the data subject

The right is subject to fewer conditions and data subjects can request more extensive information concerning:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients to whom the personal data have been or will be disclosed; the period for which the personal data will be stored;
- the right to rectification, erasure, restriction or objection;
- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to their source.

TWO FOUR ONE FOUR

Section 3: Rectification and erasure

Article 16: Right to rectification

The data subject shall have the right to the rectification of inaccurate personal data:

- right to have incomplete data completed;
- Including by means of a supplementary statement

Section 3: Rectification and erasure

Article 17: Right to erasure (‘right to be forgotten’)

Data subjects have the right to the erasure of personal data where one of the following grounds applies:

- the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation;
- the personal data have been collected in relation to the offer of information society services.

Section 3: Rectification and erasure

Article 18: Right to restriction of processing

The data subject shall have the right to restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject,
- the processing is unlawful, and the data subject opposes the erasure of the personal data, and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the original processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Section 3: Rectification and erasure

Article 20: The right to data portability

The data subject has the right to have personal data transmitted to another data controller

- Data controller must provide the data subject with a copy of personal data in a structured, commonly used and machine-readable format;

- Data controller must not hinder transmission of personal data to a new data controller;

- The right of data portability only applies where:
  - data is processed by automated means; and
  - the data subject has provided consent to the processing; or
  - the processing is necessary to fulfil a contract

Section 4: Right to object and automated individual decision making

Article 21: Right to Object

The data subject shall have the right to object to:

- processing of personal data for direct marketing;
- processing of data for profiling;
- processing of data by automated means;
- processing for scientific or historical purposes.

Exceptions:

- The controller must demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.
- The processing is necessary for the performance of a task carried out for reasons of public interest.

Section 5: Restrictions

Article 23: Restrictions

Controllers and processors may, by EU or Member State law, be restricted in applying specific articles where it is a necessary and proportionate measure to safeguard:

- national security;
- defence;
- public security;
- all activities related to prosecution of criminal offences;
- economic or financial interests of the Union or of a Member State, including public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected with the aforementioned activities;
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

Module 4

Data Controllers and Processors

Section 1: General obligations

Article 24: Responsibility of controller

- Implement appropriate technical and organisational measures;
- Implement data protection policies;
- Adhere to codes of conduct to demonstrate compliance.

Section 1: General obligations

Article 25: Data protection by design and by default

- The controller shall implement appropriate technical and organisational measures.

- Only data necessary for each specific purpose is processed.

- The obligation applies to the following:
 - the amount of data collected;
 - the extent of the processing;
 - the period of storage;
 - the accessibility to that data.

- Personal data is not made accessible to an indefinite number of natural persons without the individuals intervention.
- Pseudonymisation and Minimisation are recognised techniques in data protection by design.

TWO FOUR ONE FOUR

Section 1: General obligations

Article 27: Representatives of controllers or processors not established in the Union

Where the controller or the processor are not established in the Union:

- They shall designate in writing a representative in the Union; Representative shall be established where data processing or profiling resides;
- The representative shall be mandated to be addressed by supervisory authorities and data subjects for the purposes of the Regulation; Designation of representative does not absolve controller or processor from legal liabilities.

Section 2: Security of personal data

Article 32: Security of processing

A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:

- pseudonymisation and encryption of personal data;
- ensure the ongoing confidentiality, integrity and availability of systems;
- a process for regularly testing, assessing and evaluating the effectiveness of security measures;
- security measures taken need to comply with the concept of data protection by design;
- take steps to ensure that any natural person working for the controller or processor only processes data under explicit instruction unless required to do so by EU or Member State law.

Section 2: Security of personal data

Article 33: Notification of a personal data breach to the supervisory authority –

- Introduction of mandatory data breach reporting;
- Data controllers obliged to report security breaches to the relevant supervisory authority without undue delay;
- Where feasible, not later than 72 hours after they first become aware;
- If not made within 72 hours, a justification for the delay must be provided;
- Not necessary to notify where breach is “unlikely to result in a risk for the rights and freedoms” of data subjects;
- Processor shall notify the controller without undue delay after becoming aware of the personal data breach.

Section 3: Data protection impact assessment and prior consultation

Article 35: Data protection impact assessment

- DPIA must be performed where processing is likely to result in a high risk to the rights and freedoms of natural persons.

- It shall contain at least:

- a description of processing and operations;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks;
- compliance with approved codes of conduct;
- whether data subjects have been consulted.

How can 2414 Group help?

- GDPR Consultancy
- GDPR Staff Education
- Cyber Security Assessment (CDCAT)
- Security as a Service
- Follow on training; GCHQ Certified Cyber Security Professional (GCCSP), COBIT5, ISO27001, 9001, Agile Project Management (AgilePM), SCRUM

Remember 5% returning customer discount and 10% referral finders fee***

- Consultancy; ISO9001, ISO27001, Cyber Essentials Assessments, Business and Management

***Referral fee only counts when a booking is received and confirmed

TWO FOUR ONE FOUR 2414