QUOSTAR

GDPR Quick Start Guide.

Your guide to all the key terms you need to be aware of in the run up to the official start of the GDPR.

ACCOUNTABILITY.

The new accountability principle in Article 5(2) requires that you comply with the principles and states explicity that this is your responsibility. You must take a proactive, systematic and answerable attitude towards data protection compliance, and put in place comprehensive but proportionate governance measures.

ANONYMIZATION.

A data protection tool whereby personal data is stripped of any identifiable information, making it impossible to identify or derive insights on an individual, even by the party that is responsible for the anonymization.

BIOMETRIC DATA.

Any personal data which relates to the physical, physiological or behavioural characteristics of an individual, and allows them to be uniquely identified.

BREACH NOTIFICATION.

Following a personal data breach you must notify the relevant supervisory authority and the individuals concerned (where the breach is likely to result in a high risk to their rights and freedoms). A breach notification must contain: the nature of the data breach, the name and contact details of the data protection officer, a description of the likely consequences of the personal data breach and a description of the measures taken - or proposed to be taken.

CONSENT.

Under GDPR consent must be freely given, specific, informed and unambigious indications of the individual's wishes. There must be some form of positive opt-in showing they agree for their personal data to be processed, consent cannot be inferred from silence, pre-ticked boxes or inactivity.

DATA CONTROLLER.

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose for which and the manner in which personal data is processed.

DATA MINIMISATION.

The idea that, subject to limited exceptions, an organisation should only process the personal data it actually needs to process in order to achieve its processing purposes.

DATA PROCESSOR.

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

DATA PROTECTION IMPACT ASSESSMENT (DPIA).

Also known as Privacy Impact Assessments or PIAs. These help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. A DPIA must be carred out when you are using new technologies or the processing is likely to result in a high risk to the rights and freedoms of individuals.

DATA PROTECTION OFFICER (DPO).

A mandatory security leadership role required by the GDPR. A DPO is responsible for all data protection activities within a business including, but not limited to, strategy and implementation, business and employee education and training, and public requests regarding personal data. They are the primary point of contact for the supervisory authority and are responsible for communicating information about personal data breaches. The role of DPO can be allocated to an existing employee, providing there is no conflict of interest, or can be outsourced, but the person should have professional experience and knowledge of dataprotection law.

DATA RELATING TO CRIMINAL OFFENCES.

Data relating to criminal convictions or offences may only be processed by national authorities. National law may provide exemptions subject to suitable safeguards.

DATA SUBJECT.

The individual the personal data relates to.

ENCRYPTED DATA.

Also known as cipher text, encrypted data is data which has been translated into another form or code which is only accessible/readable to those who have the decryption key or password. When decrypted with the correct key the data is viewable in its original format.

GENETIC DATA.

Data concerning the inherited or acquired characteristics or an individual which reveals unique information about the health or physiology of that individual.

LEGAL PERSON.

Is an individual, company or other entity which has legal rights.

LEGITIMATE INTERESTS.

The right a company has for contacting an individual based on their judgement that the individual will legitimately want (or need) to receive that information. It is a bit of a grey area.

NATURAL PERSON.

In legal terms, a natural person is a person that is an individual human being.

PERSONAL DATA.

Any data which relates to an identified or identifiable natural person. This could include data such as a name, identification number, location data or an online identifier.

PERSONAL DATA BREACH.

A breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data. It is more than just losing personal data.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Any piece of data which allows you to identify an individual.

PRIVACY BY DESIGN.

An approach to projects which takes privacy and data protection into account throughout the whole process. Although this approach has always been recommended by the ICO, Article 25 of the GDPR identifies “privacy by design” and “privacy by default” as specific obligations. It requires data controllers to implement appropriate technical and organisational measure so that, by default, only the personal data which is necessary for each specific purpose of the processing are processed.

PROCESSING.

Anything you do to personal data is classed as processing. This includes, but is not limited to recording, structuring, storing and analysis.

PROFILING.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.

PSEUDONYMIZATION.

A privacy-enhancing technique design to reduce the risk of identification to a data subject. It involves processing personal data in such a way that it cannot be attributed to a specific individual without the use of additional data. The additional information must be kept separately and securely from the processed data to ensure the data subject cannot be identified.

RIGHT TO BE INFORMED.

Your obligation to provide "fair processing information", typically through a privacy notice. It emphasises the need for transparency over you use individuals' personal data. It must be written in clear and plain language, be transparent and concise, and be easily accesible and provided free of charge. The amount and type of information you supply is determined by whether or not you obtained the personal data from the individual.

RIGHT TO DATA SUBJECT ACCESS.

Under GDPR individuals have the right to obtain confirmation that their personal data is being processed; access to their personal data; and other supplementary information. This is information must be supplied to the individual free of charge and within one month of receiving their request.

RIGHT TO ERASURE.

Also known as the "right to be forgotten". Enables an individual to the request the deletion or removal or their personal data where there is no complelling reason for its continued processing, they withdraw their consent or the data was unlwafully processed. It does not provide an absolute "right to be forgotten" and there are some specific cirmcumstances where the right to erasure does not apply and you can refuse the request.

RIGHT TO OBJECT.

Individuals have the right to object to processing based on legitimate interests of the performance of a task in the public interest/exercise of official authority; direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics.

RIGHT TO PORTABILITY.

Allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

RIGHT TO RECTIFICATION.

Individuals are entitled to have personal data corrected if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties you must also notify them of the rectification, where possible. .

RIGHT TO RESTRICT PROCESSING.

Similar to rights outlined by the Data Protection Act, individuals have a right to "block" or suppress processing of their personal data. When processing is restricted you can store the personal data but not process it further. You must retain just enough information about the individual to ensure that the restriction is respecteed in the future.

SENSITIVE PERSONAL DATA

Personal data which reveals racial or ethnic origin, political opinions, religious or political beliefs, trade-union membership, data concerning health or sex life and sexual oientation, genetic data or biometric data.

SUPERVISORY AUTHORITY.

The independent public authority who will be enforcing the GDPR. In the UK this is the Information Commissioners Officer (ICO).

QuoStar Solutions
Waverley House, 115-119 Holdenhurst Road,
Bournemouth, BH8 8DY
+44 (0)845 644 0331
info@quostar.com
www.quostar.com

QUOSTAR