NEOPOST

Send.Receive.Connect.

The Neopost Guide to Managing GDPR

Smart Ways to Manage the new General Data Protection Regulation

FOR HR PROFESSIONALS

NEOPOST

Introducing our guide to managing GDPR

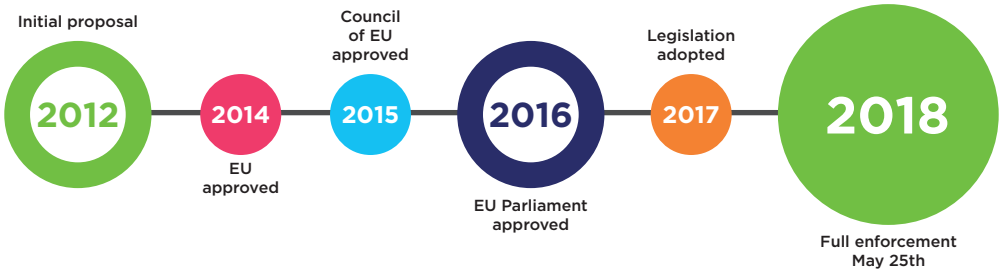
The General Data Protection Regulation introduces significant changes to existing data protection laws. The onus of GDPR is firmly fixed on giving greater empowerment to individuals, regarding the personal data that is held on them.

This guide has been written to help organisations in both their understanding of GDPR and some practical actions that can be taken, in order to ensure their readiness going forward. Particular focus is given to managing subject access requests and compliant communications.

GDPR has been around for some time

Many people may be unaware that the road to GDPR has been an extensive one. The journey commenced back in 2012 and the legislation is live now. However, the key date to be mindful of is 25th May 2018, as this date signifies when the legislation will become fully enforced.

Organisations need to consider what data is held on individuals and their future rights, in terms of access to this data and how it needs to be managed going forward. Although much of the available information focuses on the significant penalties for non-compliance, the real priority should be ensuring that robust processes are in place to both protect personal data and manage the new requirements, the legislation brings.



IF YOU'RE NOT GDPR COMPLIANT YOU COULD BE FINED UP TO

4% OF GLOBAL TURNOVER

OR CAPPED AT

€20,000,000

WHICHEVER IS THE HIGHEST

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

GDPR comes fully into force 25th May 2018

On this date GDPR fully replaces the existing data protection framework, under the EU Data Protection Directive. Organisations involved in processing personal data of any sort will need to be aware of how the regulation addresses them directly and the obligations it imposes.

The GDPR and you

It is essential that all organisations immediately start preparing for the implementation of GDPR by carrying out a review of any personal data (anything that can be used to identify an individual) being processed. This will allow time to understand the current position and look to ensure that adequate processes are in situ.

Risk of greater penalties

Although the financial penalties are significant, in that the maximum fines for non-compliance have increased to 4% of global turnover or €20,000,000 (whichever is greater), consideration must also be given to the other aspects of risk.

Breaches under GDPR are likely to create significant negative PR, which can be highly detrimental to brand equity and corporate reputation alike. Perhaps more significantly, however, is the risk to trust in your organisations by customers, suppliers and other stakeholders.

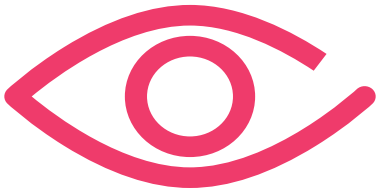
Key considerations

There are many considerations around GDPR, but some key elements include:

1. The legislation has been designed to regulate personal data processing.
2. Regulations have been constructed to encompass the growth in digital technology.
3. BREXIT and the triggering of Article 50 will not affect the implementation of GDPR.

Organisations will need to demonstrate that they are adopting a 'data protection by design' philosophy

THE GDPR EMPHASISES



TRANSPARENCY

SECURITY

AND ACCOUNTABILITY BY DATA CONTROLLERS

NEOPOST

Is your organisation ready for GDPR?

In order to better understand where your organisation is, with regard to readiness for GDPR, we have created a few vital steps to follow:

Review your current data position

Assess and audit all customer personal data that exists within your organisation. This should help you better understand what data is held and what processes are in place to create and manage it. You should also consider how data is used, across the organisation and how it is protected. Any data that does not serve a functional purpose should be minimised or deleted entirely.

Put together a team

This needs to be led from a senior level. You will need a team of subject matter and process experts, in order to fully understand the data held in your organisation.

The size and scope of your organisation will determine the size of the team required, in most cases. Your team will help review, implement and manage change in line with the requirements of GDPR. It is important that all findings are evidenced, to meet compliance requirements.

In other words, DOCUMENT EVERYTHING!

Appoint a data protection officer

A team is a great place to start getting your organisation ready, but someone will need to take overall responsibility.

For some organisations, GDPR requires that they appoint a Data Protection Officer (DPO), but for those out of scope it still makes sense to appoint someone to take the lead. This role should report directly to senior management and manage the overall position within the organisation.

The three instances in which a DPO **MUST** be appointed are:

1 If you are a public body (excluding courts acting in their judicial capacity).

2 If you carry out large scale systematic monitoring of individuals.

3 If you carry out large scale processing of specialist categories of data, or data relating to criminal convictions and offenses.

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

Update your privacy policies

Focus on GDPR's demand for transparency and ensure your data policies reflect this. It is important to place the spirit of privacy at the heart of all policies. Organisations should also consider any impacts from interactions with others, such as suppliers and external data processors working on your behalf. The communication of policies is also important, these should also be transparent, documented and written in plain English.

Get technical with data protection

Investment in technology and expertise play an important part in getting ready. What can be done with internal processes to protect your customers' data? You should also consider if there is anything that can be done with the data itself, to make it more secure.

This aspect also touches on requirements to encrypt and anonymise data held within the organisation.

Communication is key

Building additional compliance will be academic, if no one knows about it. Employees need to be fully informed and engaged, in order to understand their individual responsibilities in meeting compliance requirements.

From a commercial standpoint, your customers are likely to be looking for peace of mind and this can create competitive advantage and potential business opportunities as a result.

Plan for more communication

GDPR is a dynamic approach to data protection and is ready to adapt to future changes in the digital landscape. Plan ahead to update your policies, to reflect any future changes in the legislation.

It is also a good idea to use simple, regular communications to inform those that need to know of the actions you have taken.

NEOPOST

How can Neopost help you get ready for GDPR?

With this guide, we have aimed to produce a simple document with straightforward advice and practical actions that organisations can take, to help in the preparation for the full implementation of GDPR.

There is a tremendous amount of noise on the topic out there. The complexity and scale of the legislation means that often some of the advice can also be complicated and unclear.

There are a number of organisations out there promising utopia, or resolving all worries associated with GDPR. This is not an approach we adopt, nor indeed endorse. We have elected to take a different approach, focusing on relevant areas in which we have specific knowledge and expertise.

THE LEGISLATION ITSELF IS MADE UP OF

99

DIFFERENT ARTICLES, WHICH IN TURN ARE BUILT FROM

451

PARAGRAPHS

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

The Neopost approach to getting GDPR smart

Our approach concentrates on some of the key areas of GDPR. For ease of understanding we have categorised our areas of expertise into four segments. These segments are Amendment, Communication, Consent and Process.

NEOPOST

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

The Neopost approach

To help get your organisation ready, we will now expand on these areas and relate them directly to the requirements of key articles within the wider GDPR legislation. It is in these areas that we can help.

ARTICLE 15

Right of Access

PROCESS

This Article relates to managing requests from customers and other stakeholders, about the data you hold on them. Anyone is entitled to issue such requests to your organisation, under this Article. They may request confirmation that data is held on them and being processed, access to the personal data you hold and other associated information.

In dealing with such a request it should be noted that typically the requestor cannot be charged for dealing with the request. It should also be noted that you have just 28 days to respond to such requests.

How Neopost can help

Neopost offers robust solutions around data management. With regard to Article 15, we can provide a technology platform to consolidate data from around your organisation. Simply export your data set into the technology platform, which can interrogate the data, identify and consolidate all information relating to the individual making the request.

Once the data has been consolidated for that individual, or output management solution can take this information and format into a pre-designed template. Once created, the finished document can be sent to the individual, either through multiple channels (paper or digital) based on the requestor's preference.

It should be noted that information requests are all encompassing. As well as data that is held in systems such as your CRM or customer databases, it also pertains to information that is held on paper. Neopost technologies can also manage this requirement, by digitising paper based information so that it can also be exported to create a holistic view of customer information, should you have the requirement, the data extraction process can be automated, using Robotic Process Automation.

ARTICLE 16

Right to Rectification

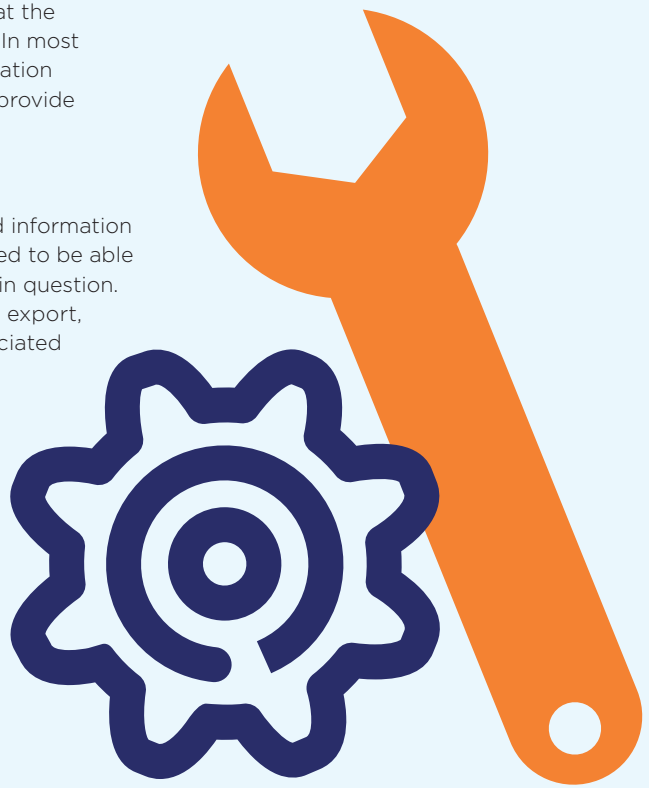
AMENDMENT

An individual has the right to request that information held on them is amended or rectified without delay. This also means that any data held that is incomplete, must be completed as part of the request. There is a time limit of 28 days that relates to the completion of any requested amendment, that organisations must adhere to.

Once data has been rectified, the legislation also states that the data subject must be informed that the rectification has taken place. In most cases, the request for rectification will follow from a request to provide information on the data held.

How Neopost can help

In order to rectify and amend information held on an individual, you need to be able to access all the information in question. By performing a similar data export, we can help identify all associated records on the individual. Having done so, it is a simple case of identifying the information that needs to be amended.



NEOPOST

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

The Neopost approach

ARTICLE 17

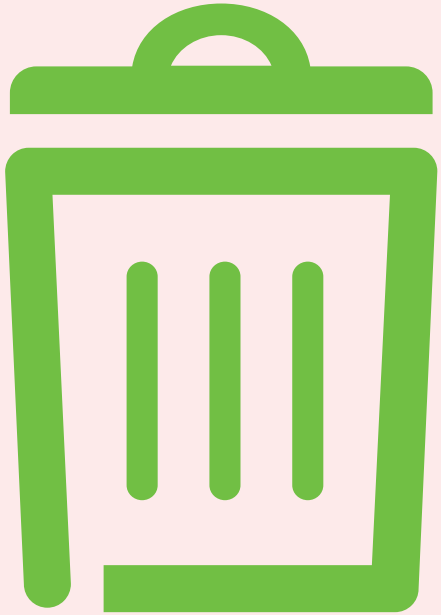
Right to Erasure

AMENDMENT

The Right to Erasure is also known as the Right to be Forgotten. The broad remit to this article is that any individual has the right to request that any data held on them is deleted. It should be noted that this Article must be adhered to only if there is no compelling reason for the data to be held.

How Neopost can help

The Neopost solution to Article 17 follows a similar path to the right to rectification. An organisation can export data into our technology platform, where the same de-duplication and consolidation is achieved. Having consolidated all data on the subject, and in the context of there being no compelling reason for it to be held, this data can be identified for deletion from the holding system(s).



ARTICLE 18

Right to Restriction

CONSENT

This Article relates to requests from individuals for data not to be processed by your organisation. Where a request has been made to rectify personal data, you restrict the usage of that data until the appropriate amendments have been made.

Having exported the information and found the areas for amendment, you will be aware of customers for whom data processing should be restricted. Often the restriction relates to not sending communications to that individual.

How Neopost can help

Neopost output management solutions can be utilised to add such an individual to a 'DO NOT MAIL' list. Once created, any communications addressed to that individual can be blocked from being sent.

As well as relating to individuals that have made data access requests, this same solution can be used to manage consent. Any individuals that have not given explicit consent for you to communicate with them, for marketing purposes for example, the same 'DO NOT MAIL' list can be used as cross reference.

When creating any communication run, our software will cross reference against the 'DO NOT MAIL' list to ensure that the individual concerned is not sent the communication piece.

NEOPOST

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

The Neopost approach (cont)

ARTICLE 19

Notification Obligation

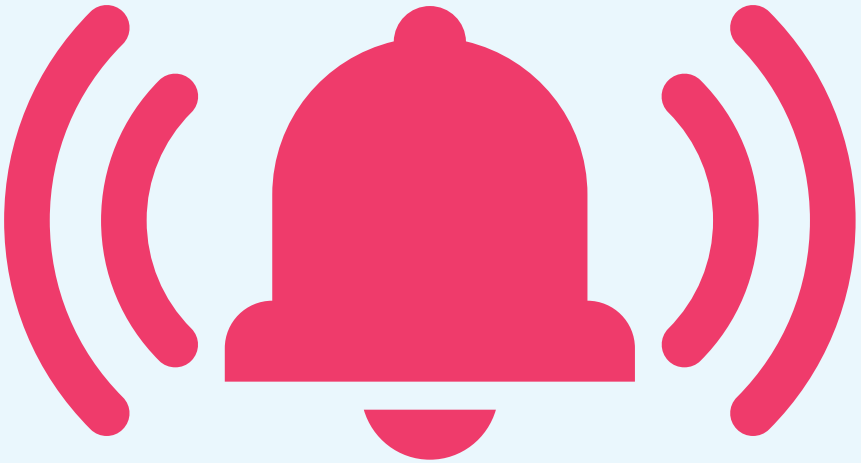
COMMUNICATION

There are two strands to this particular Article. Firstly, any changes made to personal data by the organisation must be advised to the data subject.

By working alongside your database or CRM systems, a flag can be created in order to identify changed records. Our output management solution can then look for such a flag and hence understand individuals for whom a change has been made.

How Neopost can help

Once identified, the individuals' contact information can be exported to a standard document template advising them of the change. This can then be sent physically or digitally through the same technology platform.



ARTICLE 25

Data Protection by Design

PROCESS

This Article can be viewed as being all encompassing. In essence GDPR states that an organisation processing and controlling data must build data protection by design into its internal processes. In order to be compliant with the legislation, an organisation must be able to evidence the specific steps it has taken to build data protection compliance into its processes.

How Neopost can help

For an organisation that has invested in the Neopost GDPR technologies, such evidence can be easily provided. By simply deploying the technology within your organisation, you have already taken steps to make your internal processes more compliant.

In the event of any investigation, the usage of such technologies should be cited. The investment will go some way to proving that you have taken appropriate steps to compliance within your organisation.

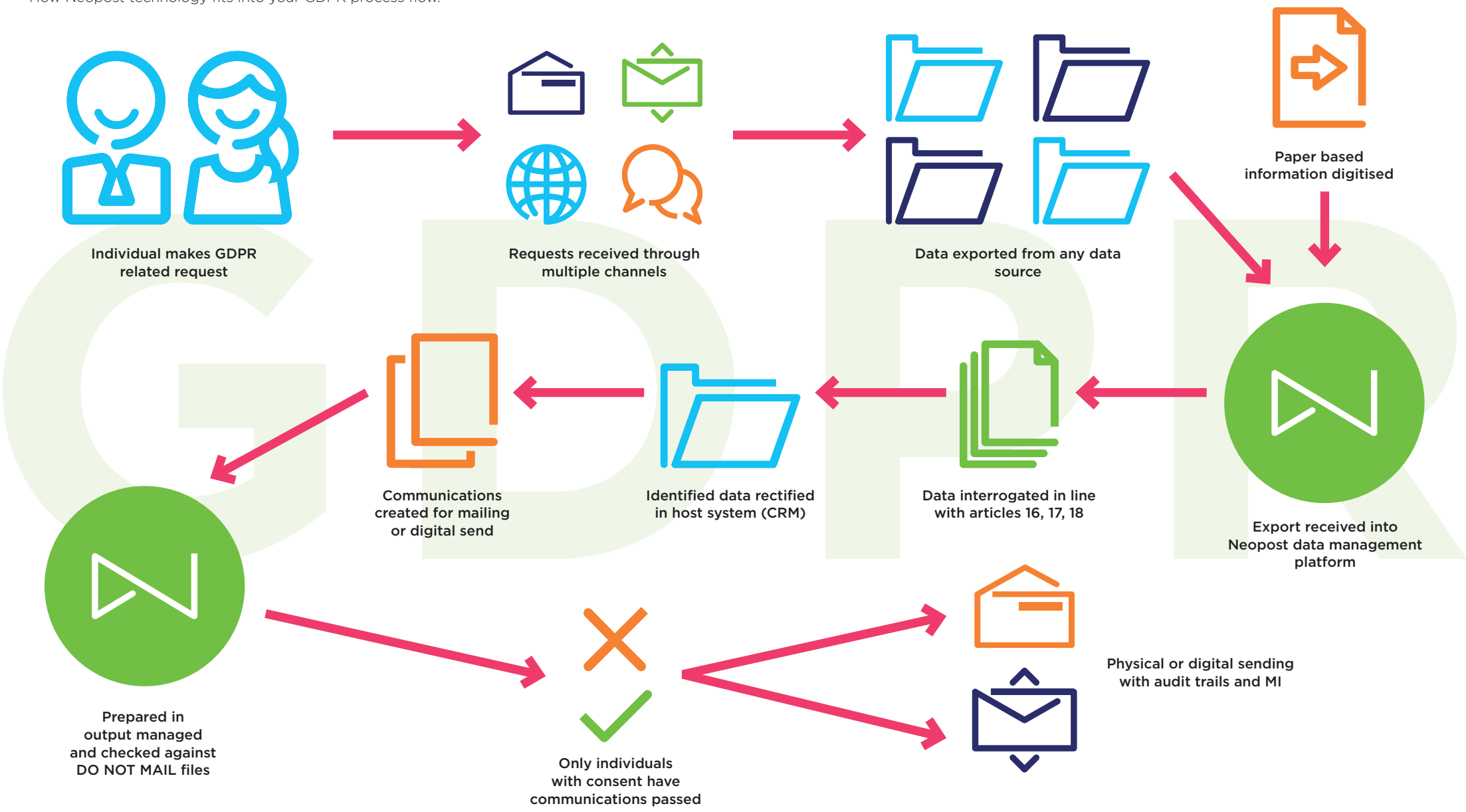
NEOPOST

If you need any further information on managing GDPR visit: www.neopost.co.uk/GDPR

GDPR TECHNOLOGY SOLUTIONS BY NEOPOST

Neopost GDPR Technology Solutions

How Neopost technology fits into your GDPR process flow.



NEOPOST

GDPR GLOSSARY OF TERMS

Binding Corporate Rules (BCRs) - a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)

Biometric Data - any personal data relating to the physical, physiological, or behavioural characteristics of an individual which allows their unique identification

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

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

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, 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 Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

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

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - 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

Delegated Acts - non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity

Derogation - an exemption from a law

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 - 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

Genetic Data - data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual

Group of Undertakings - a controlling undertaking and its controlled undertakings

Main Establishment - the place within the Union that the main decisions surrounding data processing are made; with regard to the processor

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

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

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.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

Recipient - entity to which the personal data are disclosed

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

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

Right to be Forgotten - 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

Trilogues - informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.

If you need any further information on Neopost services and products, please call **0800 0855 367** (quoting GDPR) or go online to: **www.neopost.co.uk/GDPR**

Neopost Limited
Neopost House, South Street, Romford, Essex RM1 2AR.