nathean

General
Data
Protection
Regulation

GDPR What You Need to Know...

Prepare for the General Data Protection Regulation with Nathean Analytics

Organizations can be fined up to 4% of annual global turnover (or €20 Million) for breaching GDPR so not having a process in place to ensure compliance could prove to be a very expensive mistake! Is your organisation ready?

What does GDPR Mean?

GDPR, or the General Data Protection Regulation, is an EU regulation which updates the existing Data Protection Directive aiming to simplify, unify and increase the protection of personal data.

Enforceable from **25 May 2018,** this EU regulation differs from the original Data Protection Directive which was enacted in 1995 prior to widespread adoption of the internet. which has transformed the way we create, use, share, and store data.

As a *directive*, the existing framework could be implemented by member states as they saw fit, resulting in different approaches to data protection across Europe. GDPR is a *regulation* and as such must be followed much more rigidly, and not just in Member States: the regulation affects any organisation who collects or uses the personal data of EU residents.

What is Personal Data?

Under the new regulation, any information related to a natural person or 'Data Subject', which can be used to directly or indirectly identify that person is considered "Personal Data".

It can be anything from a name, a photo, an email address, a phone number, a National Insurance (NI) number, bank details, posts on social networks, medical information, or a computer IP address.

Key Points:

- **All organisations holding personal data on EU Residents** will have to comply with the requirements of GDPR – even those in non-member states.
- **A Data Protection Officer must be nominated** in all Public Authorities and any company where core activities require monitoring of data subjects.
- **There must be a valid reason to collect or use** Personal Data.
- **Clear and affirmative consent** of the individual must be obtained for the collection or use of their data in an **intelligible and easily accessible form.**
- **Data processing registries will become mandatory** A record of personal data processing activities, covering the lifecycle of the data, must be kept.
- **Privacy by Design** calls for the inclusion of data protection from the first stage of designing new systems, rather than an addition.
- **Privacy Impact Assessments** will be required for technology or processes that are likely to be high risk to the individuals, for example data profiling.
- Any data breach must be reported to the local data protection authority **within 72 hours.**
- Organisations must provide data subjects with an **electronic means of making access requests**, which must be responded to within one month, free of charge and in a commonly used file format.
- **Individuals gain the right** to correct inaccuracies, have information erased and exercise greater control regarding how their data is used.

For more information on Nathean Analytics, please contact us on:
T: UK +44 (0) 1275 377 200 / IRL +353 (0) 1 685 3001 **E:** info@nathean.com
www.nathean.com

10 Steps to Prepare Your Organisation for GDPR

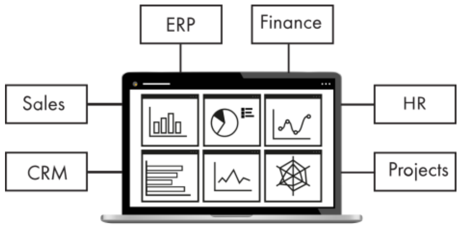
If your organisation holds, or processes, the personal data of residents of the European Union, you need to ensure that key staff are aware of the new regulation and begin to identify areas that could cause compliance problems.

Your Data Protection Officer should ensure that:

1. An inventory of all personal data you hold is created and examined to determine how it was obtained, why it's being held, how long it will be retained for and how securely it's held.
2. Current Data Privacy notices are updated to reflect the new regulations and written in concise, clear language.
3. Procedures are reviewed to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format
4. Procedures are in place to handle data access requests within the new timescales
5. That a legal basis exists for holding or processing any personal data your organisation holds
6. Customer Consent to recording of their data has been 'freely given, specific, informed and unambiguous' and that you can demonstrate this consent was given (i.e. an effective audit trail must be in place).
7. Adequate systems are in place to verify ages and gather consent from guardians where personal data relates to underage subjects.
8. You have adequate procedures in place to detect, report (within 72 hours unless data was anonymised or encrypted) and investigate a personal data breach.
9. Data Protection Impact Assessments (DPIA) are carried out where high-risk processing is being undertaken
10. Service settings are automatically privacy friendly, and any new services and products being developed take account of privacy considerations from the outset ("privacy by design" and "privacy by default")

How can Nathean Analytics help?

While no software package can make an organisation GDPR compliant, there are tools which can make the role of Data Protection Officer less onerous!



Nathean analytics' self-documenting, federated approach to Business Intelligence provides Data Protection Officers with an out-of-the box inventory of data sources it's connected to and an easy way to identify personal data.

Self-service reporting and analytics tools improve business user's ability to respond to data subject access requests within one month and in commonly used electronic formats.

Nathean Analytics' embedded Spreadsheets module empowers users with all the flexibility of Microsoft Excel™ in a governed, secure, browser-based environment. This greatly reduces the risk of data loss from local copies of personal data being held on employee laptops or omitted from responses to subject access requests due to data isolation. To learn more visit www.nathean.com