General Data Protection Regulation

GDPR essentials and how PwC can help

EU Data Protection rules set to change

The EU General Data Protection Regulation ("GDPR") imposes a radical, much tougher data protection regulatory framework on Europe and the wider world for the processing of personal data. Every EU-based "controller" or "processor" of personal data is regulated, as is every controller based outside the EU that targets goods or services at, or profiles, people living in the EU.

Understanding processing

The idea of processing is very broad. It covers every processing operation that can be done on personal data, irrespective of whether it is undertaken by automated or non-automated means or whether done actively or passively. The initial collection of personal data right through to its final deletion or destruction is considered processing, as is creating personal data; storing; using; copying; aggregating; adapting; amending; sharing; transmitting; archiving; selling; losing; and erasing the data.

The use of email to communicate, as an example, will constitute processing personal data. Every email we send in business relates to at least one person and, therefore, sending an email will involve the processing of personal data. The generation of computer logs as we use our work systems, or our personal devices will involve processing personal data also. Payment transactions when we shop on the high street or online will do so too. The recording of CCTV footage and the spoken word also involves the processing of personal data. Processing even occurs through the giving of feedback on our colleagues at appraisal time. Virtually every technology device and database that is used in business processes personal data in some way.

The GDPR requires that controllers and processors of personal data shall act lawfully, fairly and transparently in their use of personal data and how they deal with the people to whom the data relate. Controllers have to be open and honest about what they are doing and why. They cannot, for example, mislead people about why they are using their data. Controllers have to stick to the purpose for which they acquired the data, minimise the amount of data held, keep it accurate, up to date and secure and confidential at all times, they must then delete it or destroy it when the purpose for which it was obtained or created is fulfilled, or if consent to use the data has been withdrawn. People who ask questions about what is happening with their data are entitled to answers and to be given copies of that data. If they have good grounds to ask for processing to stop, then stop it they must.

pwc

The big innovations in the GDPR

The adoption of the GDPR will present many entities everywhere with numerous new challenges. Key issues to be aware of include:

Compliance
Strict new compliance requirements will be imposed. For example, entities will have to perform "Privacy Impact Assessments" and privacy audits as a matter of course. They will have to implement "Privacy by Design" methodologies into their business, so that compliance is baked-in to everything they do. They will have to deliver on a new "Accountability" obligation, which means creating written compliance plans, which they will have to deliver to regulators on demand.

Usage controls
Personal data will be subject to strict new usage controls. These include "data minimisation", "data portability" and "right to be forgotten" principles, which will require entities to limit the use of data, to enable individuals to take their data with them at the end of a relationship and to delete and destroy data on request.

Consent
Obtaining consent to use personal data will be much harder to achieve and to prove.

Bundling
The provision of a service that is conditional upon the individual giving permission for their data to be used for non-essential purposes (such as marketing) will be banned.

Aggregation
The ability to aggregate data to enable an individual to be profiled (a common objective in new digital projects) will be severely curtailed.

Supervision
Regulators will also be empowered to carry out audits and inspections of entities on demand.

Breach disclosure
Entities will be required to report serious contraventions of the law to the regulators and to people affected. Public disclosure of failure is likely to fuel regulatory sanctions and compensation claims, as well as causing damage to brand and reputations.

Fines
Serious contraventions of the law will be punishable by fines of up to either 4% or €20 million of group annual worldwide turnover.

Litigation
Citizens and pressure groups have the right to engage in group litigation ("class actions") to recover compensation for mere distress caused by contraventions of the law.

A funnel is created to more disputes and litigation – breach disclosures

Part of the challenge of the GDPR is that it creates a funnel through which non-compliance turns into serious regulatory penalties, litigation and public disgrace. The funnel is the breach disclosure requirement, which will effectively require entities to "wash their dirty linen in public". Breach disclosure laws were invented in the United States where they have fuelled regulatory mega-fines and mass litigation.

Pinch points

The features of business that are most affected by the GDPR are:

- Consumer facing activities
- Activities relating to children
- Marketing and advertising
- Digital transformations
- Geolocation
- Profiling
- Tracking
- Public services
- Mass communications
- Joint ventures
- Global business operations

The need to prioritise

The GDPR raises countless compliance issues. It would be very easy to "get lost". Work needs to be prioritised, so that critical risks issues and key business objectives are addressed before matters of lesser importance.

The "legalistic" approach –v- the "risk based" approach to compliance

The legalistic approach to GDPR compliance focuses simply on the legislative requirements within the GDPR, without any weighting for risk, or the entity's key business objectives. Generally speaking, the legalistic approach will deliver the same compliance programme shape for all entities.

The risk based approach recognises the operational realities of business and the way the law is enforced in practice. The risk based approach recognises that, in the real world, businesses, litigators and regulators have to make hard choices about their priorities. It will therefore tackle major risk areas first, taking account of the entity's key business objectives, and it will seek to maximise return on investment, by re-utilising previous works. The risk based approach requires a more holistic view of the issues than the legalistic approach.

Optimised programme design, to deliver a risk based approach and a holistic view

Optimum programme design begins with the statement of a Vision for the entity's desired End State. The Vision is the articulation of the entity's aims and objectives, which provides an ongoing reference point for the work over time, to ensure that the business priorities are kept fully at the forefront. The Strategy for the compliance programme has to be fully aligned with the Vision. Once the Strategy has been developed, the entity can establish the Structures that are necessary to support the Vision. Many entities rush to begin work on Structures, however, rather than spending sufficient time considering Vision and Strategy. This is a key problem of the legalistic approach.

How PwC can help

As a multi-disciplinary practice, we are uniquely placed to help our clients adjust to the new environment. Our data protection team includes lawyers, consultants, auditors, risk specialists, forensics experts and strategists. Our team is truly global, with on the ground expertise in all the major EU economies.

Compliance requirement	*Professional services skills required*
Accountability and Privacy by Design	Strategy, business transformation, compliance programme design, advisory work (including legal advice), controls and assurance
Privacy Impact Assessments	Risk advisory and assessment services
Privacy audit	Audit services
Breach Disclosure	Incident response and legal services
Regulatory supervision	Legal services and supporting expert professional services