AurigaConsulting

Cyber-smart – business savvy
Applying business expertise to keep your information systems safe

10 ways GDPR
will change your business

Many companies today are claiming to be GDPR experts in a period of huge uncertainty. Auriga is considered by its customers as the authority on GDPR due to its EU GDPR Practitioner status.

What makes GDPR different to standard compliance regimes is the need to embed or bake-in the required processes and not just add some additional checks and balances. GDPR is a business process modelling exercise where organisations are required to assess, unpick and build in a number of comprehensive processes.

According to Dell...

80% of 821 global organisations

polled said they knew little or nothing about the GDPR.

and...

97% said their companies didn't have a plan

in place to implement the new regulation.

plus...

with penalties hitting an upper limit of €20 million or 4% of annual global turnover

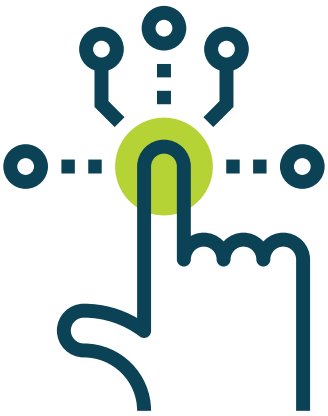
whichever is higher, the stakes are high. This is particularly concerning when you consider the complexities of embedding such a process.

So how can Auriga help and where do we have experience?

Let's start by exploring some of the key areas of concern and expand on Auriga's capability in those areas...

10 ways GDPR **will change your business**

1 What's new?



Today's online world is very different, compared to when the Data Protection Act (DPA) was created. To accommodate this new world, GDPR delivers greater rights for data subjects and greater obligations for the data controller and organisations. They will demonstrate accountability including data sharing and the accuracy of personal data.

Auriga's experienced GDPR analysts deliver:

- **an efficient and focused business process assessment**
- **concise documentation highlighting where and how personal data is processed**
- **mapped processes creating a fundamental roadmap of the data's journey, interaction points and parties including system details. This part of the process spans:**
  - **Contracts**
  - **ICT systems**
  - **Personnel/roles**
  - **Governance**

Auriga utilises this foundation phase to assess an organisation's GDPR capability.

2 Planning

Key planning for GDPR requires raising awareness by contacting key people and areas of your business, highlighting key decision makers, perhaps at board level and exploring existing governance capabilities.

Auriga offers complete end to end GDPR delivery including communication and project management capabilities which reduces the burden of GDPR delivery from the organisation to allow them to concentrate on what they do best.

3 Communication

GDPR also requires the communication of privacy notices, letting people know how their data will be used. This wide requirement contains much more information such as timescales, complaints procedure and the clarity of information within the privacy notice.

Auriga can assist organisations in planning and embedding these procedures to allow your organisation to meet the communication obligations to ensure you are never in breach. Auriga's customers find this particularly helpful especially within heavily complex and integrated systems.

4 Privacy means business

Individual rights build upon the DPA and enhance the privacy capabilities afforded to the individual.

- Subject access rights
- Accuracy
- Prevention of profiling
- Prevention of direct marketing
- Rights to erasure
- Right to deny direct marketing
- Right to portability to allow people to move to different service providers

Just considering how an organisation handles requests for deletion and the tracking of that information can create serious challenges!

Auriga delivers a GDPR compliant set of processes which ensures the data controller can accommodate requests from people to access the data. In most cases this must be free so must be efficient for your organisation to comply with. Timescales will also become more stringent, reduced from 40 days to 1 month.

Auriga works with its customers to embed and "bake-in" the subject rights to ensure every one of our customers' processes and systems along the data flow are compliant.

These seemingly simple personal data rights have a huge impact on existing systems and processes.

5 No more tick boxes

Legal basis for processing and storing personal data must be explicit – organisations must understand the legal basis for them processing personal data, document and communicate the basis. Consent will be unambiguous and explicit whilst clear standards of consent must be adhered to and must be driven by a positive confirmation from individuals. No longer will simple tick boxes be sufficient as we have become used to.

As part of its GDPR compliancy service, legal basis for data processing is comprehensively considered as part of the data life-cycle. This can seem simple, but when Auriga works with its customers' complex and integrated systems, residual data can be discovered which would be a breach under GDPR, particularly within historical and accounting data.

6 Parental consent

The processing of children's personal data requires parental consent. Organisations who process children's personal data must start to determine how their systems will meet and accommodate the parental consent which must be verifiable.

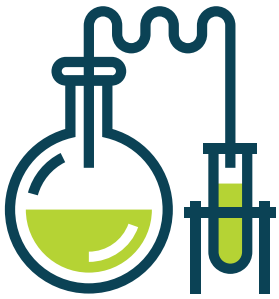
Auriga delivers this specific requirement for its customers as part of its business process exploration phase. Children's data or systems particularly focused on children will be defined and remodelled from a GDPR consent perspective with minimal impact to the existing business.

7 72 hours

Data breaches must be recorded by the Information Commissioner's Office (ICO), by the data controller as well as the individual in question within 72 hours.

Auriga assesses, remodels comprehensive, complex integrated systems and builds in these seemingly simple requirements remembering to consider the customer's data flow and life cycle. Reporting mechanisms are a fundamental part of GDPR!

8 Baking!



Data protection by design must be at the forefront of system and process designers whilst data protection must be intrinsic to systems and processes instead of being an afterthought. Authorisation from a data protection authority like the ICO would also need to be obtained if the results of the privacy assessment do not sufficiently identify acceptable controls.

Auriga always works with its customers to ensure GDPR requirements are "baked-in" and are not an afterthought!

9 All the way to the top!

Data protection officers must be considered to conduct systematic monitoring of data privacy requirements. The status of the individual or body must have high or board level reporting mechanisms as well as consideration for influencing policy and procedural changes.

Auriga looks at existing roles and responsibilities and makes maximum use of existing personnel. Often, personnel will need to be trained in the complex field of GDPR - ask Auriga for further details!

10 25.05.2018

Borderless data privacy approaches must be maintained. By the 25th of May 2018 organisations who process data on behalf of EU citizens will be included within the scope of the regulation.

International organisations do not escape GDPR if they are not on EU soil. If they process EU citizen data they are within the scope of GDPR.

Utilising its wealth of experience, Auriga can assess and scope the requirements, impacts and size of the task. Contact us today for more information! www.aurigaconsulting.com +44 (0) 20 3793 8820