A.C.T
Consulting you can trust

ACT: Delivering GDPR Compliance

GDPR in a nutshell

Richard J Hannah

Richard is a former Data Privacy Lawyer, who spent 15 years with the big four consultancies. He is part of the GDPR Institute, GDPR Awareness Campaign, was on Data Protection Act Derogations committee and served within UK Government within the Cabinet Office. The original 'GDPR in a Nutshell Article' has had over 7,700 hits and reposts. He worked on the DPA 1984.

This service description describes our approach to supporting organisations to achieve compliance to GDPR. The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') will enter into force in May 2018. It will create a single law on data protection across the EU. It will have a significant impact on organisations in Europe as well as any organisation (wherever situated) that may hold data on Europeans. This data may be customers, business partners or employees. If you simplify the rights to the individual that GDPR introduces it is simply this:

1. You must get consent to hold data on a person, and you must explain why you hold that data and for how long;

2. A person can ask you for information you hold on them and you are obliged to provide it. Information includes written and digital records;

3. A person has a right to demand that you remove their details from your records;

4. If you transfer data outside your borders it must be anonymised and of course protected.

The challenge is that there are few exemptions other than the obvious - defence, police, NHS and the Media. Organisations that hold data to meet their legal obligations (or fulfil a statutory purpose are **not exempt** from the Act. They simply do not have to comply with requests to **remove** details or **ask consent** to hold data. They must however comply with all other aspects of GDPR. GDPR replaces 20-year-old Data Protection Legislation. It introduces legislation with significantly more powers to punish non-compliance. The Regulator will have powers to impose significant fines for non-compliance of up to 4% of annual **worldwide** turnover for a corporate group. Non – Commercial organisations will face fines, reputational damage and of course compensation claims from those impacted. It is anticipated that 'PPI' style agencies will switch from targeting PPI claims (which end in 2019) to claims for compensation under the new laws.

So, what does this mean for your company?

With only a few months to go until the GDPR becomes law, organisations should now seriously consider the impact of the GDPR by carrying out a comprehensive internal gap analysis of current data privacy and cybersecurity practices as compared to GDPR requirements. We set out below some broad-brush recommendations as a starter for ten:

- **Data Mapping:** In English that is map and understand, where your data is, what data is deemed sensitive and understand where your data comes from and to;
- **Understand the scope of the act:** Garner an understanding of that the GDPR applies to:
    - any EU based controller (user) of personal data and anybody who processes data on their behalf. For instance, if you outsource your IT services or transfer information to associate businesses and organisations;
    - an entity with no EU presence at all which processes the personal data of an individual in the EU. That could be an outsourced business in India or China, for instance.
- **Data Protection Impact Assessments (DPIAs)**: Data Protection Impact Assessments ('DPIAs') should be completed when using new technologies and where processing techniques are likely to result in a high risk to individuals (e.g. employee monitoring). DPIAs need to be done now for **current** activities.

- **Consent, notices and policies:** Consent is king. Providing detailed privacy information to individuals will be required under the GDPR (such as how long data is retained). To be compliant, consent must be unambiguous and specific. Separate consent is required for each use of data. This will have significant impact on organisation such as Charities, those who run Membership schemes, Local authorities and all of us who invest heavily in CRM systems. Data Brokers will need to rethink their business models.
- **Understand the new privacy rights of individuals** including rights to:
    - erasure of data (e.g., when data is no longer necessary, or consent is withdrawn);
    - object to processing, including in relation to direct marketing; and
    - data portability (i.e., transferring data to another controller where processing is based on consent or on contract performance).

Organisations will need systems to provide proof. '*Yes, we did that*' is not compliant.

- **Restrictions on profiling:** The GDPR imposes new restrictions on organisations that conduct automated decision-making, e.g. profiling (essentially any form of analysis of personal data) with some exceptions.
- **Mandatory Data Breach Reporting:** Under the GDPR, personal data breaches must be reported without undue delay to the data protection authority and where feasible within 72 hours. Where the breach is likely to result in a high risk to affected individuals they must also be notified without undue delay. Organisations should implement appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and loss/destruction of or damage to personal data.

Amending your contract Terms

Under the GDPR, we recommend your procurement contracts are reviewed and amended to contain obligations for your suppliers to:

1. assist with data subjects' rights requests;
2. notify you of data breaches; and
3. assist you with DPIAs.

If you supply a service or product, you may find your customers and business partners asking you to do the same thing.

International Data Transfers

The GDPR has a lot to say about transfers of personal data to countries outside the EEA (such as the US) that are deemed by the EU to not provide an adequate level of protection. International transfer solutions include among others:

1. Consent, that must be freely given and meet GDPR consent requirements;
2. EU Standard Contractual Clauses;
3. Binding Corporate Rules;
4. Approved Codes of Conduct or certification mechanisms; and
5. The EU-US Privacy Shield.

It's a hefty piece of legislation, don't ignore it! but see the act as an opportunity and not a red tape challenge. If businesses grasp the nettle, they can use the GDPR as a means of improving Customer Relations, Reviewing and improving commercial terms and strengthening cyber security. It provides a sharp focus on all aspects of digital transformation and business operations. Our ACT Portfolio of service will:

- Ensure you are compliant and remain compliant;
- Make the logical links to improving Cyber Security;
- Support initiatives to help defray the costs of complying with this important piece of legislation.

Delivering GDPR

The Challenge

Fundamentally, GDPR is a Business Transformation Programme. The issue for all organisations is that it is being presented as a threatening regulatory compliance programme and addressed as such. At EACS, we consider that choosing the right partner and your own leadership of the GDPR programme is extremely important.

Choose the right Programme Leadership

In our experience, the natural home for a GDPR Project should not be legal or compliance or IT because this can result in organisations focusing too much attention initially on defining policies, procedures and model contracts. The Compliance function may well be adept at is adept at highlighting risks, it is not typically responsible for making risk-based decisions. This team needs to be at the Transformation table but free to apply risk judgements and be pragmatic in its interpretation of the legislation.

We would strongly recommend that the Information Security team does not take the lead either. GDPR is not an information security programme. Security is a component of the programme and is often coupled with privacy. However, it is only one of many considerations required for GDPR compliance. GDPR is a programme about changing behaviours, which in turn leads to operational and technology changes in most aspects of your business:

- HR
- Technology
- Digital Transformation
- Customer Services
- Information Security
- Compliance
- Legal and Commercial
- Archiving and administration

Traditionally, these types of programme are difficult to execute across an organisation in any industry, let alone when the clock is ticking, and the regulator is anticipating many organisations will address the regulation with as light a touch as possible. No matter, who you choose as your service partner in this area, you need to select a leader supported by a team drawn from all impacted areas, with the capabilities and authority to impact change across the extended organisation.

Selecting the right DPO will be the key to GDPR compliance success for many organisations. In most cases, the DPO will not be the person currently fulfilling the role under existing legislation. The GDPR creates many new obligations for the DPO. The person in this position must have:

- An understanding of what it takes to run an enterprise wide programme and the authority to make the changes necessary to embed appropriate controls in business processes.

- The ability to apply sound judgement and make risk-based decisions quickly to meet reporting deadlines.

- The ability to drive change in the organisation and establish a defensible strategy for deployment.

Other Considerations

We recommend that organisations keep the following considerations in mind when developing their GDPR compliance programme:

- The GDPR will be disruptive to your portfolio of programmes. GDPR requirements will have a significant impact on planned initiatives;

- Organisations should look to create complementary initiatives in each of the impacted areas to defray the costs of implementing this programme. This should include reviewing legacy systems, introducing infrastructure optimisation programmes and reviewing web sites and CRM technology - the Programme must be paid for!

- Organisations will find themselves spending significant resources on digital transformation programmes only to find they cannot derive the anticipated value due to restrictions arising from the GDPR. Therefore, organisations should consider not only current activities, but also future activities that may form a part of digitalisation initiatives;

- This Programme is not a one hit and done programme. It is exactly like any other change programme - it is all about continuous improvement. Therefore, the complete management of the GDPR life Cycle year in and year out must be invested in and added to annual running costs;

- Brexit adds complications. Far from exempting companies from complying with the GDPR, as many companies have hoped it would, Brexit will complicate matters for many organisations that are subject to GDPR. The UK Government has led the creation of this legislation, the timetable for the GDPR will run ahead of any formal exit by the United Kingdom from the EU.

The UK Government generally supports the GDPR and its underlying principles and its official guidance to organisations is therefore to "press ahead" with GDPR compliance;

- Finally, the legislation impacts electronic/digital and manual paper records. Document Management is now front and centre in the war on data privacy.

Supporting companies to meet the challenge

Working with our strategic partners, our response is to create the industry's most complete portfolio of GDPR related services. We consider we have a solution to meet most of the challenges, GDPR Presents and the know how to work with you to meet those challenges unique to your organisation. Our approach is a straightforward one following our own framework. Clients can take as much or as little assistance as they need, our multi-disciplined teams and our GDPR related toolset are deployed around your need.

This example framework is supported by technology tools and software solutions that the Client may or may not choose to implement. Our approach is as follows:

STAGE	DESCRIPTION	BENEFIT
Strategy Review	Complete review of your existing strategy	*Understand company direction and culture and identify any potential conflicts*
Assessment	Gap analysis of 'as is' versus obligations under GDPR	*Understand GAP before committing to complete project*
Statement of Works	Create complete Scoping and Programme charter document. Get Scope signed off	*Understand Scope and socialise impending changes*
Plan	Comprehensive plan including dependencies and conflicts with existing initiatives, set up governance, initiate comprehensive Communications plan	

Compliance	Complete Compliance implementation	*Complete Compliance activities according to plan*
Life Cycle Management	Build Life Cycle management platform	*Build tools to manage breaches, requests for information and data privacy activities*
Return on Investment	Initiateinitiativestopayfor programme	*Ensure bottom line not impacted by completing initiatives to deliver GDPR programme*

As well as consultancy we offer a range of complementary technology solutions to support our transformations:

- **Data Privacy Information Portal** with advice available to the DPO on relevant data privacy law across Europe (12 months licence);
- **GO Pro** - Compliance Life Cycle Management Tool to manage GDPR (and any other compliance issues);
- **GoVerify** – Anti-phishing software
- **Secure@source**: Sensitive data mapping and monitoring, data anonymization tools for cross border data transfer.

Project Central

Project Central is at the centre of our execution and contracting strategy, bringing together fundamental activities aimed at protecting planning and budgeting without compromising Project quality and the integrity of client strategy. Our Projects (and by extension our Clients) benefit from an environment which integrates the disciplines of planning, contracting, resource management design and contractual deliverables with document management, team collaboration, reporting and performance management during the project lifecycle.

The complexities of today's capital projects, operating in the digital environment and project teams drawn from consortia and different geographies, brings its own challenges. Our response is to place our Project Central teams at the heart of our Project Management, Programme governance supporting a unified, collaborative project environment supporting all key disciplines and all phases.

Using the Project Central solution enables us to better collaborate and share project content and deliverables in a more controlled, managed environment. We provide our clients with bespoke reports, SLAs, Contract management workflows and visibility into project costs and risks for financial performance monitoring and reporting.

What Project Central does:

- **Gain project and performance insights:** See exactly how individuals and contractors are contributing on a project. Key performance indicators show the state of your deliverables and reveal bottlenecks. You will see exactly what action is required, and by whom. Then, measure project completion based on current progress and trends;
- **Manage and control documents:** Go beyond simple document management to full document control. Accurately manage, distribute, and archive data and information in context across multiple data repositories. Connect all relevant content required to ensure delivery of reliable asset information throughout the project lifecycle;
- **Manage contracts and mitigate project risks:** We proactively identify and track risk items to help minimise potential delays and plan for contingency. Create risk items instantly, link them to documents and communications, and view them on your risk register;

- **Manage design content:** Integrate and manage engineering, architectural or technology design content. Enable effective control and change management for designs, documents, project deliverables, and other related information types. Increase productivity and team efficiency by managing all content in a single, unified environment;
- **Manage compliance:** Ensure compliance with your organisation's corporate records policy. With advanced file plan and disposition control, all records and associated information are integrated in a comprehensive information model making manual declaration unnecessary. This approach gives visibility to all records throughout the lifecycle for assurance and compliance;

- **Resolve issues:** Speed the reliable resolution of issues discovered by project team members and/or stakeholders;
- **Track change orders and other requests:** Track your contractors' and consultants' schedule of values, pay estimates, and change-order proposals electronically. Simply review and approve these documents and your financial reports are automatically updated.

Meet the Team

Our GDPR practice comprises a cadre of Senior Professionals who are deployed around our clients' needs and offer a combination of disciplines. GDPR implementations require professionals with Legal, regulatory, Programme management and Change management skills and our Senior Management Team reflects this:

Richard Hannah, Principal Data Privacy Consultant: Richard was a Data Privacy Lawyer who can trace his experience back to the committee stages of the DPA 1984. He is a published author of a string of often referenced white papers. His recent reprint of 'GDPR in a Nutshell' received over 7000 reads on LinkedIn, over 600 positive comments and Likes and has become required reading in organisations across Europe. He is an in-demand key note speaker and a member of the GDPR Institute, The GDPR Awareness Campaign in Ireland and is the architect of our Data Privacy by Design Service. Richard has over 40 years of Consulting experience including 15 years as with global consultancies Capgemini, Capita and Accenture. His personal assignments have included work at Chelmsford City Council, HMRC, CAA, TUI Group, London Borough of Harrow. This team has worked with Richard on multiple assignments since 2000.

Andrew Beattie, Head of Transformation Programmes: Andrew is responsible for the smooth delivery of all our Transformation and Programmes. Formerly with Capita before joining the business full time in 2017. He is a highly proficient Director and leader with a wealth of experience in managing outsourced operations and delivering large-scale programmes both in the public and private sectors. Key areas of expertise and competency as follows: Programme and project management Change and transition management Business development and sales Contract negotiation Business management and delivery Building and developing relationships at CxO level Continuous improvement Cost efficiency Trouble shooting Contact centres Solution design.

May Ladd, Head of Information Security & Regulatory Compliance: May is a subject matter expert, senior consultant and trainer in Document Management, Enterprise Content Management (ECM) Records Management, Information Architecture, Information Security and Compliance, Big Data. He has 20 years Consulting experience. His recent assignments include: Cambridge University, Deutsche Bank, Credit Suisse, TeliaSonera, Bank of England, Ministry of Defence and Tullow Oil. He leads a practice that includes consulting in Document Management, Records Management Systems, ISO15489, EDRM, Enterprise Content Management (ECM), Information Security, ISO27001, Information Compliance/Risk/Architecture, Big Data, Taxonomy, Data Protection Act, General Data Protection Regulation (GDPR), Scanning, Workflow, Digital Asset Management, Enterprise Search, Archiving and Preservation, Information Management & Compliance.

Trevor Scott, CISO: Trevor is one of industries most experienced CISO (and CIO Consultants). He has worked across industry recently at Cambridge University, William Hill and Thomson-Reuters. He worked with Richard Hannah at Fujitsu and completes assignment globally. Though technically Dr Trevor Scott, this is no theoretical Executive consultant he roles his sleeves up as CISO to complete activities routinely such as:

- Developed and implemented procedures to ensure safety of employee and visitors.
- Ensured that all computer systems were properly protected
- Carried out daily security procedures
- set risk assessment standards and reviewed regular reports assessing risk
- investigated possible security breaches and worked to restore any data lost
- developed and implemented emergency procedures to deal with security threats
- Developed risk management assessments
- managed digital and physical security
- Assisted with periodic internal security audits

Martin Sanderson, Senior Information Consultant: Martin specialises in information, records and knowledge management and their implementation. He was an information manager for the NHS to 1985 and then Consultant for the World Health Organization 1985-1988. He has over 30 years Consulting experience and his assignments have included work at: 3M Health Care, Boots Pharmaceuticals and BASF Pharma, UK. He has completed a lot of work in the Public and Third Sectors and is a recognised thought leader with strong domain knowledge. He is a past Vice Chair of the Records Management Society and currently a member of the Editorial Advisory Board for Records Management Journal. Since 2010 he has focussed on assignments with Government Agencies, Universities and International Organisations.

Other Practice Heads include:

- SharePoint Team Lead: **Adrian Hilder**
- ERP Implementation and Data Migration: **Robert Peledie**
- Cyber Security Team Lead: **Michael Kemp**