GDPR:
The devil is
in the data

shaping tomorrow with you

FUJITSU

A recent newspaper article chose a revealing headline: 'GDPR: the new data-protection law giving watchdogs a mega-bite.'[1]

Much of the coverage of the EU's new General Data Protection Regulation (GDPR) has been focused on the possibility of huge fines being levied on companies that fail to comply with the provisions of GDPR. But at Fujitsu we prefer to accentuate the positive.

As our key issues paper 'GDPR: Threat or opportunity?' argues, the new regulation is an opportunity. EU statutory authorities agree. They have indicated that companies which distinguish their products and services by data privacy standards will win more business.

This is not only an obligation but an opportunity. With compliance comes competitive advantage, as organizations can better utilize the data at their disposal, gain critical insights, and build trusted relationships.

This paper explains how approaching GDPR from the perspective of people, process, and technology as well as enabling digital transformation, you can make the most of the opportunity. There are six short sections:

GDPR is not about technology　〉

Focus on people　〉

Data is at the core of all businesses　〉

Understand your data, make it visible　〉

It's all part of your digital transformation　〉

People, policy and processes and technology that deliver 'privacy by nature'.　〉

[1] The Guardian: December 14th 2017

GDPR is not about technology

GDPR is about protecting the personal data of individuals. Technology will help you to do that, but the emphasis needs to be on achieving a holistic view of all the data that you hold and process. To do that you need good policies and governance. Your processes, systems and technologies then need to be aligned with those policies.

In that way, everything you do can be linked back to the basic principles outlined in GDPR, and you will be able to not only comply with the regulation, but achieve significant benefits for your business, your people and your stakeholders.

That's what we mean by the 'Devil is in the Data' – look closely at the demands of GDPR,

understand what you need to do at all levels of your organization. That's important because every enterprise is complex, and there's always a risk of data getting lost or duplicated across functions and within them.

Achieving better visibility can deliver a lot of benefits to the way you operate and the information you can leverage.

That's what we mean by the 'Devil is in the Data' – look closely at the demands of GDPR, understand what you need to do at all levels of your organization.

Focus on people

The principles behind GDPR are founded in the EU Charter of Fundamental Human Rights. In this paper we make the point that the regulation is a positive step forward for the rights of EU citizens to have more control of their personal data, and to engage with organizations which hold and process it in positive ways.

We believe that this human-centric view of GDPR should be the foundation for how organizations comply with GDPR. It's not just another regulatory demand, but a means by which better managed quality information can directly contribute to business improvements and efficiencies with people's needs and rights placed firmly at the heart of the entire exercise.

It is often hard for businesses to create a true sense of ownership when it comes to dealing with privacy issues around personal data. It's been seen as an issue for lawyers or compliance specialists. It's not considered a core part of the business. That also used to be the case for cybersecurity, but the recurrence of high-profile breaches which have affected the reputations of global organizations has transformed that mindset. It is now well understood that investment in better data governance not only delivers higher levels of protection, but also engenders trust. This is what we are seeing with GDPR which aims to give individuals more ownership and control over what's happening to their personal data, even if most people won't notice the difference in their daily lives.

Your focus needs to be on the interests of data subjects – people – employees, customers and all stakeholders. Everyone you come into contact with. Their interests are the principal focus, not just technology.

It is now well understood that investment in people's personal data engenders trust for both employees and customers.

Data is at the core of all businesses

You need to build a culture of exemplary data governance. Know what data you have, where it is, what it's for, and who has access to it, as well as how long you should keep it. Organizations need to own the responsibility for protecting the privacy of their customers and employees by designing compliant business processes, based on appropriate technology, to collect and process personal data.

Effective data governance and management needs to be considered holistically rather than in silos. In an era of cheap storage, many organizations have just stored data without really understanding whether that data is still needed. This goes against the GDPR concept of data minimization – which is to only hold the minimum amount of data required, and only for legitimate purposes.

In an era of cheap storage, many organizations have just stored data without really understanding whether that data is still needed.

Understand your data, make it visible

In a world replete with threats, a lack of data visibility and understanding represents the biggest danger for organizations, not just in terms of GDPR, but for for organizational effectiveness too.

Hackers know that personal data can be profitable, so they will attempt to steal it. And, it's not just cyber that counts: data can be lost in many other ways. Poor practices can see data lost through using unsecured Wi-Fi in public places or printing out documents and then not shredding them. Good lifecycle management of data in all its forms is vital.

As digitalization projects gather pace and IoT devices like wearable or remote sensors gather increasing volumes of data (from video to numbers to sound and biometrics) you must get ahead of the data curve.

Poor practices can see data lost through careless use of technology in public places or printing out documents and then not shredding them.

It's all part of your digital transformation

At Fujitsu, we believe that your approach to GDPR should be based not just on compliance, but also on contributing to your digital transformation. Data, as we've stressed, is at the heart of any modern enterprise. You need to embark on a journey that ensures that you know where and how to invest in locating, managing and protecting your data to its maximum potential. Complying with GDPR can kick-start this.

And it's not just about personal data. We're arguing for a holistic approach to ALL data. Make it the core of your digital future. Achieving high quality information and data management can be a differentiator in a dynamic marketplace. Seeing it in this way will help you make the investment case for a robust and creative approach to your data management and governance.

Achieving high quality information and data management can be a differentiator in a dynamic marketplace.
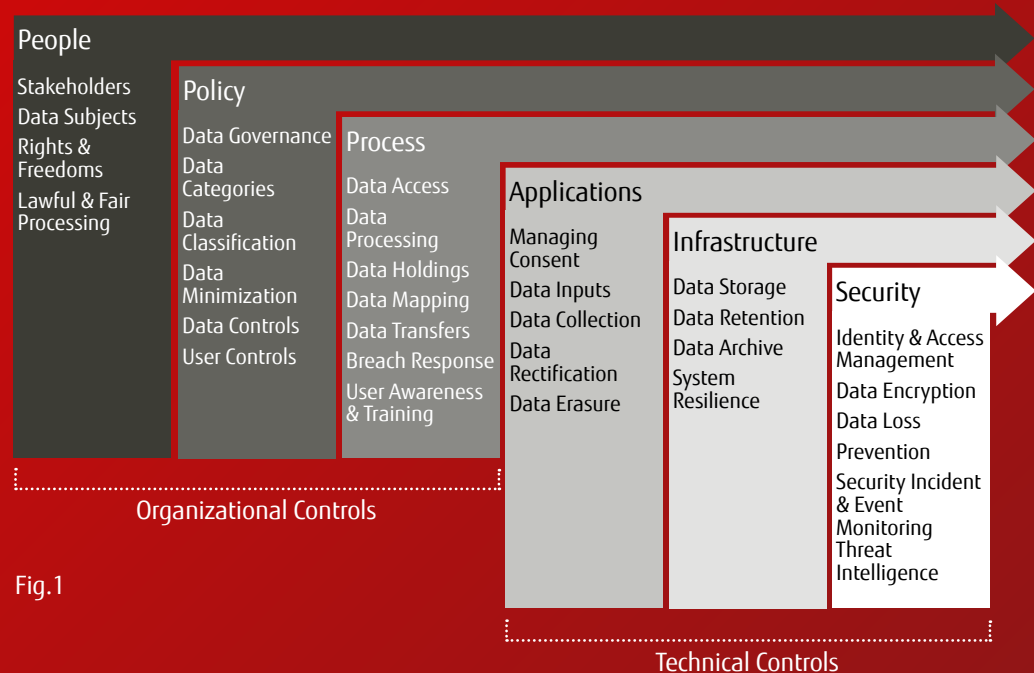
People, policy and processes and technology that deliver 'privacy by nature'.

GDPR calls for organizations to achieve its principles 'by design' which means that when they are developing, designing, selecting and using applications, services and products which are based on the processing of personal data or do so to fulfill their task, then the protection of that data must be designed into them from the start. Our approach extends that principle across everything you do to achieve what we call 'privacy by nature'.

People, policy and process are key to the former. Technical controls consist of applications, infrastructure and security. It sounds obvious, but the key is to ensure that it's all done logically, and in the right way. You need to understand the needs and expectations of all stakeholders as well as understand the rights and freedoms of data subjects (as defined by GDPR).

Understand all the categories of data you hold, and all the sensitivities associated with them. That will enable you to ensure you have categorized the data correctly and then understand what needs to be done to protect its integrity. This helps you define policies and processes. Once they're locked down, you can understand the technology you need to deploy to locate, manage and protect the data. So, for instance, you have to ensure that your systems make it possible to find personal data, extract it and, if necessary, amend or delete it. Ideally that needs to happen at the application level, and filter through to the underpinning infrastructure.

Fig.1 Sums it up visually.

Fig.1

People
- Stakeholders
- Data Subjects
- Rights & Freedoms
- Lawful & Fair Processing

Policy
- Data Governance
- Data Categories
- Data Classification
- Data Minimization
- Data Controls
- User Controls

Process
- Data Access
- Data Processing
- Data Holdings
- Data Mapping
- Data Transfers
- Breach Response
- User Awareness & Training

Applications
- Managing Consent
- Data Inputs
- Data Collection
- Data Rectification
- Data Erasure

Infrastructure
- Data Storage
- Data Retention
- Data Archive
- System Resilience

Security
- Identity & Access Management
- Data Encryption
- Data Loss Prevention
- Security Incident & Event Monitoring Threat Intelligence

Organizational Controls

Technical Controls

The end game is to ensure 'privacy by nature' – it's fundamental to what you do and who you are. That's why people are the priority. To achieve that balance of people, policies and processes, and then achieve the right level of sophistication at the application, infrastructure and security levels takes work. For many it's not something they want to do alone. Which is where a co-creation partner comes in as well as an ecosystem.

Talk to Fujitsu about how you can make the most of the GDPR opportunity.

Contact details

Ask Fujitsu
Tel: +44 (0) 123 579 7711
Email: askfujitsu@uk.fujitsu.com
@FujitsuSecurity
Ref: 3820