HULFT Newton IT

White Paper

GDPR: Solutions for four critical issues facing IT departments

Newton Information Technology Ltd

Saison Information Systems Co. Ltd — HULFT Division

15 May 2018

Introduction

As you'll no doubt know, GDPR (The General Data Protection Regulation) takes effect from 25 May 2018.

Companies in the European Economic Area (EEA) — and those outside the region which deal with any personal data from within the EEA —must comply with GDPR from IT, legal, HR, data management and marketing perspectives.

Japanese companies, for example, must conform to the Regulation in their entities within **and** outside of EEA, if they deal in any way with the data of European citizens.

So, compliance with GDPR is clearly a vital business issue. To achieve it, legal, HR, information system, marketing, compliance and many other teams within organisations need to work closely together.

This whitepaper, co-authored by Saison Information Systems Co. and Newton Information Technology, looks at the issue from an IT perspective. It summarises the background to GDPR and outlines primary factors for IT managers to consider. It then introduces IT solutions to resolve the priority challenges GDPR poses.

GDPR background

GDPR has its roots in the European Data Protection Directive (95/46/EC) of 1995. This compelled EU countries to enact corresponding domestic laws. The UK, for instance, passed the Data Protection Act 1998.

Back then, of course, personal data was processed, stored and used far less than it is today — given the ever-increasing march of e-commerce, online banking, smartphones, analytics, social media, big data, the Internet of Things and artificial intelligence.

This era of digital transformation, with its intensive reliance on data processing, has brought with it the need for a whole new level of personal data protection. And the ever-intensifying globalisation of business has increased the difficulty of complying with the fragmented domestic laws of EU countries.

GDPR was developed to respond to exactly such issues by updating and standardising rules across the region.

Enhanced regulations

GDPR consolidates and builds on privacy protection laws across EEA countries. The areas which are now most tightly regulated by GDPR are data collection, data processing and transfer to countries outside the EEA.

Data collection

Under GDPR, you now need to explain at the outset the purposes for which you collect personal data, your policy of data disclosure to third parties, the rights of data subjects (the people to whom the data belongs) and the legal bases on which you process the data.

Data processing

All organisations are now required to establish a system for processing personal data securely and fairly. Any which employ more than 250 people or process sensitive data are also required to maintain a record of all processing activities. Sensitive data, as outlined in GDPR Article 9, includes information on racial and ethnic origin, political opinions, religious and philosophical beliefs plus information about criminal convictions (Article 10).

In addition, you must accommodate data portability and the right to erasure. And you must undertake a Data Protection Impact Assessment (DPIA) in situations where any new data processing is likely to result in an elevated risk to individuals. If you regularly and systematically process personal data on a large scale, you must also appoint a Data Protection Officer.

Transfer outside the EEA

Transfer of personal data to countries outside the EEA is allowed by GDPR (Article 45) only if the European Commission (EC) has decided the receiving country guarantees an adequate level of data protection.

Countries accepted by the EC as providing enough protection include Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

In addition, personal data is permitted to be transferred to 2,723 organisations in the United States which are signed up to the Privacy Shield framework. As of April 2018, Japan and Korea are currently negotiating with the EC around similar arrangements.

Transfer to countries which haven't been confirmed by the EC as providing adequate protection could also be allowed if the receiving organisation has appropriate safeguards (GDPR Article 46) and if the supervisory authority approves its Binding Corporate Rules (Article 47) or adopts Standard Contractual Clauses.

Penalties

Fines for infringement of GDPR could be extremely large.

There are two levels, depending on which parts of the Regulation are breached:

- up to €10 million or 2% of annual worldwide turnover of your previous financial year (in the case of a company), whichever is greater
- up to €20 million or 4% of annual worldwide turnover, whichever is greater

A large company found falling short of GDPR could be hit with overwhelming penalties in the worst cases. Given the seriousness of the consequences of infringement, the next section outlines how to operate your business in full compliance.

Key areas for attention

The Information Commissioner's Office (ICO) — the UK's data protection authority — recommends priority actions in its document 'Preparing for GDPR - 12 steps to take now'.

Although the ICO is a UK body, these steps are relevant for any organisations dealing with EEA data. They cover:

1. Awareness
2. Information you hold
3. Communicating privacy information
4. Individuals' rights
5. Subject access requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data breaches
10. Data Protection by Design & Data Protection Impact Assessments
11. Data Protection Officers
12. International

This whitepaper focuses on the most critical four of these steps as concern IT departments.

Key steps for IT departments & the IT solutions

Steps	Organisational issues	Necessary actions	Solutions
Information you hold	• Unknown data transfer processes • Lack of understanding of GDPR compliance • Holding unnecessary personal data	• Data mapping • Third party assessment	• GDPR assessment
Individuals' rights	• Absence of systems to protect data subjects' rights • Lack of understanding of personal data locations	• Implementing a personal data location finder • Implementing a data management system	• Personal data locator
Data breaches	• Absence of measures to prevent & detect data breaches • Lack of breach reporting to data subjects & supervisory authorities	• Implementing data breach detection systems • Data breach logging	• Data breach detection & prevention • Data extraction • Data integrity checks
Data Protection by Design	• Inadequate security within IT infrastructures	• Scrutiny of IT infrastructure • Implementing countermeasures to address data vulnerabilities	• IT infrastructure audit • Layered information security measures

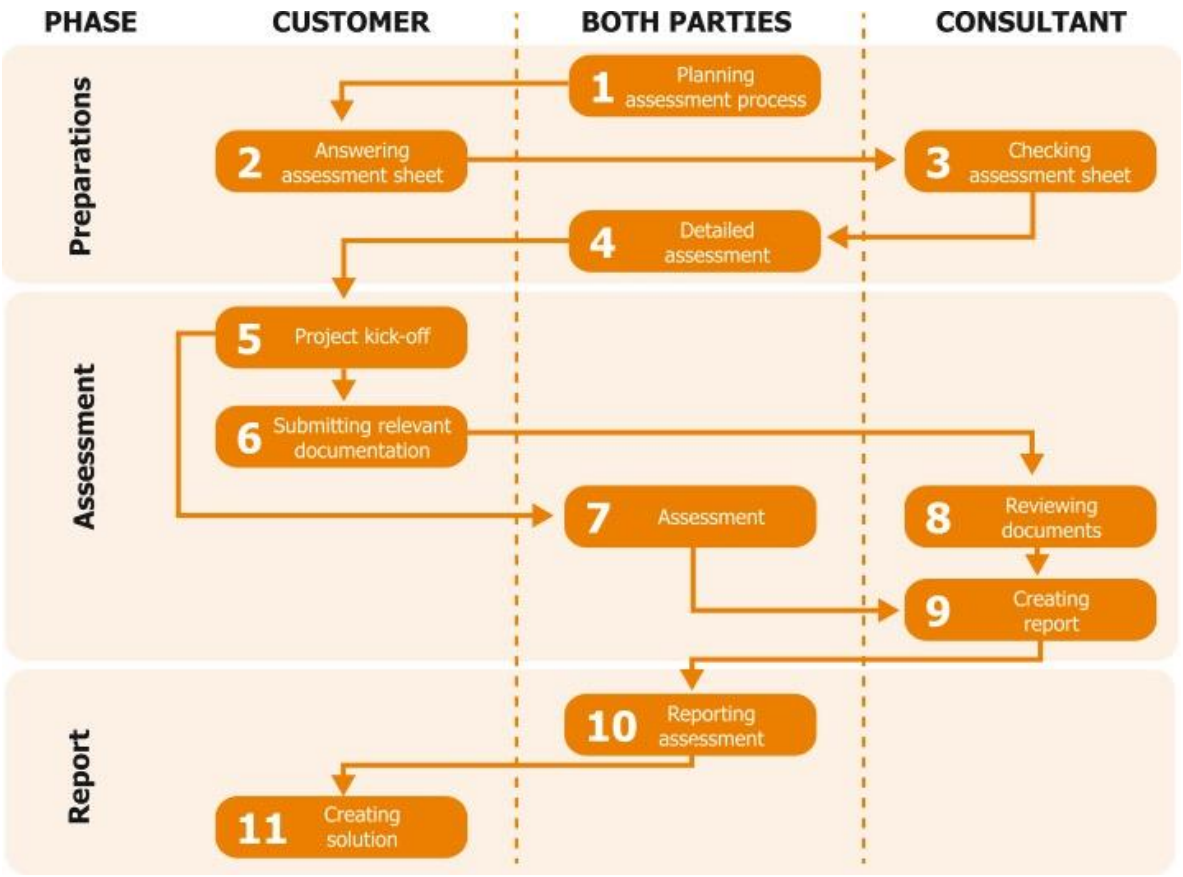
1. Information you hold

We recommend the following initial actions — which we call a 'GDPR assessment':

i. Data mapping: clarifying data types, locations, processes, data volumes and the transfer status of the personal data you hold

ii. Listing problems: documenting GDPR compliance issues emerging from the data mapping process above

The following drawing gives an example of the potential flow of a GDPR assessment:



You should prioritise the problems uncovered by the assessment and create an action plan to address them.

2. Individuals' rights

GDPR's Article 17 relates to the 'Right to erasure', Article 20 defines the need for data portability and Article 22 deals with concerns about data profiling by artificial intelligence and analytics.

In essence, GDPR stipulates that companies must safeguard the rights of data subjects. For instance, there may be a time lag between updating personal information on a business social network such as LinkedIn and updating a personal CV. Such a lag may cause a company to misunderstand information. GDPR requires such inconsistencies to be addressed urgently.

It also demands that requests from data subjects for the disclosure, removal or updating of their personal data must be handled within an appropriate time. This may need data controllers to develop systems which effectively pin-point the locations of certain data.

Automated monitoring by data integration tools could remove the manual workload involved in finding personal information. For instance, DataSpider from Saison Information Systems Co. has a 'database trigger' which can update one database instantly as soon as another is updated.

3. Data breaches

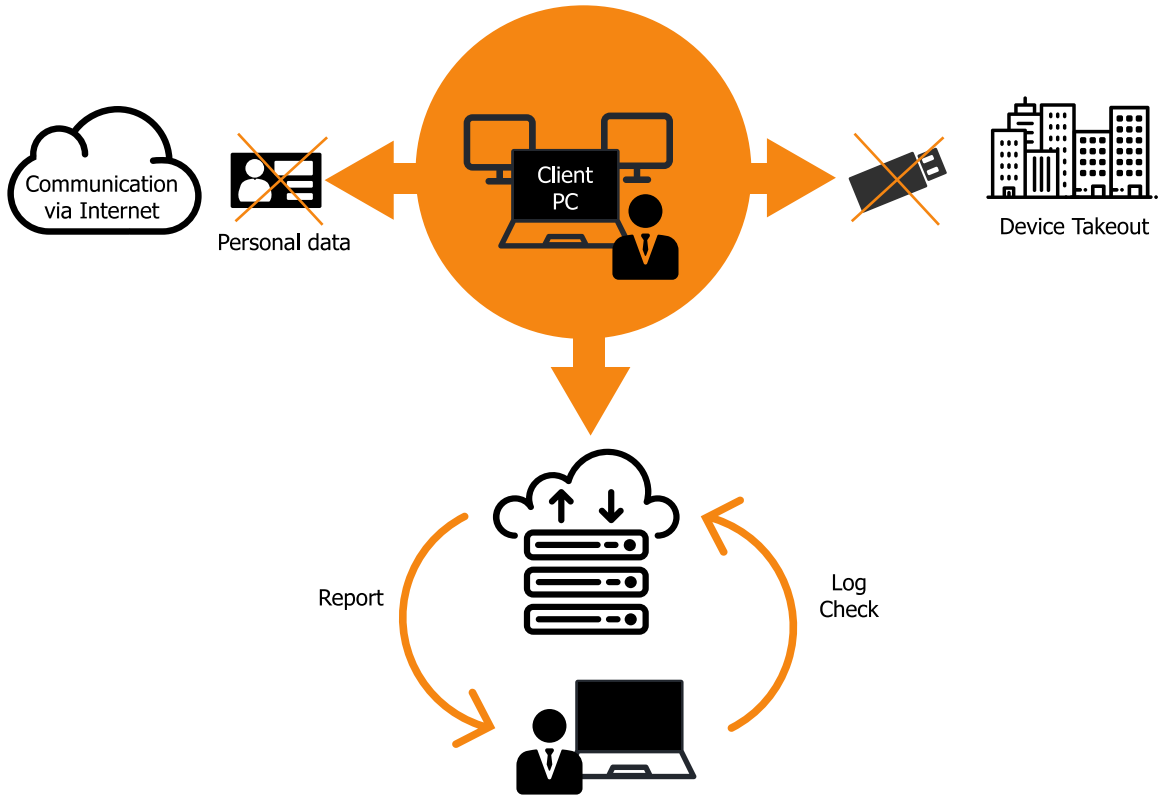
In the case of a personal data breach, GDPR requires the data controller to report the following information to a supervisory authority within 72 hours:

- the nature of the breach
- the categories of data concerned
- the approximate number of data subjects affected

It's tempting to think data breaches won't happen to you, but there are so many cases where organisations have suffered huge problems of this kind.

Regardless of the amount of data in question, it's important to put in place countermeasures for the worst-case scenarios.

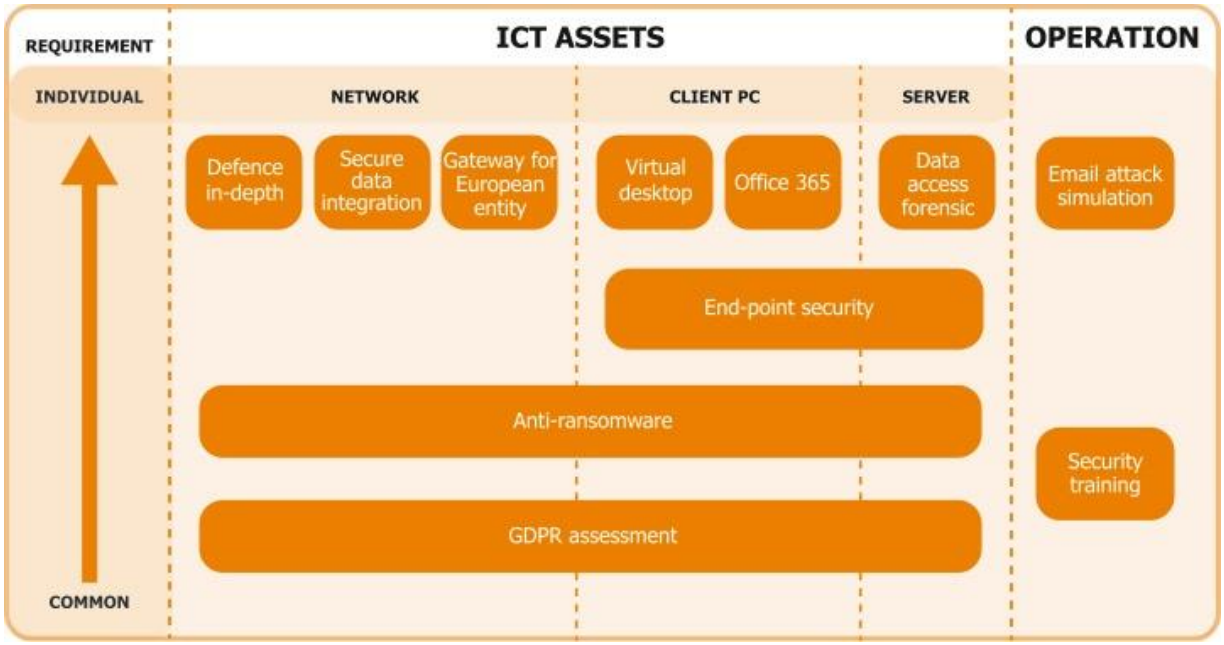
The following illustration gives an overview of a data breach detection solution:



This solution detects a breach and, if it arises, blocks the transmission of personal information through a client PC. It also logs and reports the breach to the administrator to help address GDPR's 72-hour report rule.

4. Data protection

Organisations must implement solutions to solve any issues emerging from a GDPR assessment or security audit. In terms of IT, the following are practical solutions.



Defence-in-depth

Defence-in-depth includes measures against intrusion such as firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS).

It also includes further damage mitigation (e.g. countermeasures in end-points, separation of important servers), protection against data breaches (e.g. data takeout control, data encryption) and so on. It's an approach which builds a robust barrier against unauthorised data access and theft.

Secure data integration

Because data exchanges between EU and non-EU countries are at risk of breaches, highly secure, reliable data integration with rigorous logging is necessary.

For instance, the HULFT file transfer middleware, developed by Saison Information Systems, provides AES encryption, resending of data from the checkpoint and transfer logging in one single package.

Virtual desktop

A virtual desktop environment in a data centre strengthens the security of the client IT environment. This enables IT managers to control permissions on applications for every user, apply security patches and maintain security across an organisation.

In addition, such solutions can enable you immediately to remove personal data from local devices to prevent breaches when devices are lost.

Anti-ransomware measures

Such solutions block unauthorised encryption of personal data by malicious third parties and backs up the data for disaster situations.

In the worst-case scenario, ransomware can shut organisations down and force them to rebuild PCs entirely from scratch. Solutions to ensure fast recovery are amongst the most effective countermeasures for such crises.

Gateway for European entities

European entities can strengthen the security of Internet use through cloud-based proxies. These reduce the threats from dangerous web content by restricting web browsing and enforcing secure browsing in line with your organisation's security policies.

Office 365

Office 365 ensures email security by providing email spam detection and protection.

Data access forensics

This service collects and analyses data access logs in file servers, AD (active directory) servers and database servers. If your security requirements include log management, the service can respond and prevent internal fraudulent activity.

End-point security

The combination of anti-virus software and asset management can greatly strengthen end-point security. Data Loss Prevention (DLP) features monitor and block breaches of data stored in the end-point.

Email attack simulations

This service simulates targeted email attacks to help you raise awareness amongst end-users of the importance of security.

Security training

This also helps your end-users understand the threats facing your organisation and the importance of security measures.

Conclusion

The best solution for GDPR depends on the nature of your business, the kind of data you collect, the way you use it, how you transfer it and so on.

It's vital that the solution you implement is robust and practical. We hope the points outlined above provide some helpful guidance and we will update this whitepaper as appropriate as GDPR takes effect.

Contact us

If you would like any further IT advice to help you manage the requirements of GDPR, please get in touch:

HULFT

Saison Information Systems Co. Ltd

T: +44 (0)7873 983 155

E: SalesSupport_EMEA@hulft.com

W: www.hulft.com/en

Newton IT

Newton Information Technology Ltd

T: +44 (0)20 8782 1920

E: hello@newtonit.co.uk

W: www.newtonit.co.uk

Disclaimer: *The contents of this whitepaper are based on information available to Saison Information Systems Co. Ltd and Newton Information Technology Ltd at the time of writing.*

It is designed for readers' information and to provide guidance to manage the workload of accommodating GDPR. It does not give legal advice. Organisations preparing for GDPR must understand the relevant laws and regulations as well as IT solutions and should consult legal specialists as well as IT providers.

Trademarks:

- "Office 365" is the trademark or registered trademark of Microsoft Corporation.
- "HULFT" and related products names are trademarks or registered trademarks of Saison Information Systems Co., Ltd.
- "DataSpider", "DataSpider Servista" and "DataSpider Cloud" and related products names are trademarks or registered trademarks of Saison Information Systems Co., Ltd. Other names of companies, products, and services are trademarks of their respective companies.