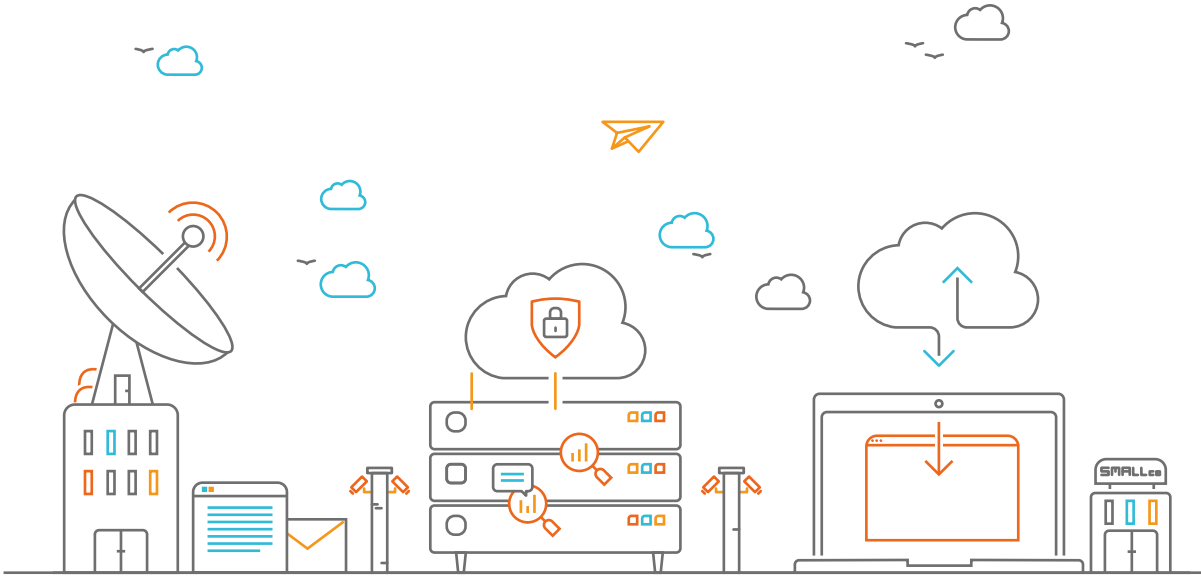
ENSURE YOU'RE COMPLIANT WITH THE GDPR

itlab



CONTENTS

You **are** in the technology business.

Whatever your mission, you need the right technology. We empower ambitious organisations to succeed.

Take the journey with us.

INTRODUCTION

The new General Data Protection Regulation (GDPR) comes into force in May 2018.

These new regulations, relating to personally identifiable data of EU citizens, are intended to update the existing data protection laws to take into consideration the changes in technology, business models, data usage, and expectations since they were written in 1995.

In particular the new regulations aim to achieve the following...

01 **Change the focus of data protection law:**

Away from a box ticking exercise

To a culture of privacy that requires businesses to understand and mitigate the risks that they create

02 **Provide additional protection for the rights of EU citizens by expanding existing rights and creating new ones, including:**

The right to be forgotten, allowing a broad right to erasure by organisations holding their personal data

The right of data portability, allowing the citizen to easily transfer personal data between companies

03 **Ensure that personal data is securely held and managed**

Adopt a proactive approach to information security

Understand and mitigate the risks to your data, both in storage and transit

04 **Ensuring that data is lawfully processed by Organisations to demonstrate that:**

Consent has been obtained

Or that they have some other lawful grounds

Ensure that Controllers and Processors are accountable

05 **Ensuring that where consent has been given by the citizen:**

That this is freely given, specific, informed and unambiguous

If the data is of a special category, the consent is also explicit

That consent is as easy to withdraw as it is to give

06 **Ensure compliance by design and by default:**

Check your in-flight programmes meet the requirements of the GDPR

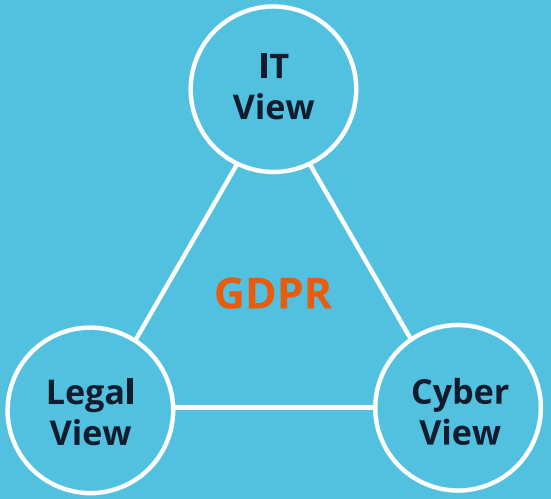
Legacy estate may require to be retrofitted to comply, or retired

The penalty for non-compliance is a maximum fine of **4% of global revenue** or **20 million EUR**, whichever is the greatest.

It is important that all companies understand the risks posed by the GDPR and how these may be mitigated. With our experience in data and process mapping, business systems, technology infrastructure and cyber security, IT Lab is well placed to support this process.

LOOKING AT THE GDPR FROM ALL ANGLES

Uniquely approaching the new data privacy law from all angles.



THE IT VIEW

The GDPR places new challenges on an organisation's technology estate and forces organisations to change the way they think about data processing.

Dan Coleby
Business Performance Director
IT Lab

The GDPR also provides them with an opportunity to tidy up the way they record, control and store client information.

Anything that gives businesses an excuse to create secure-by-design IT systems has to be a positive move.

To ensure compliance by the GDPR deadline in May 2018, organisations need to make a decision on what technologies they will invest in.

THE CYBER SECURITY VIEW

Today's cybercriminals hide in plain sight and come in many forms – premeditated hacking groups, corporate espionage, nation states and remote solo threat actors. Intelligent and determined, credible and convincing. They are also evolving.

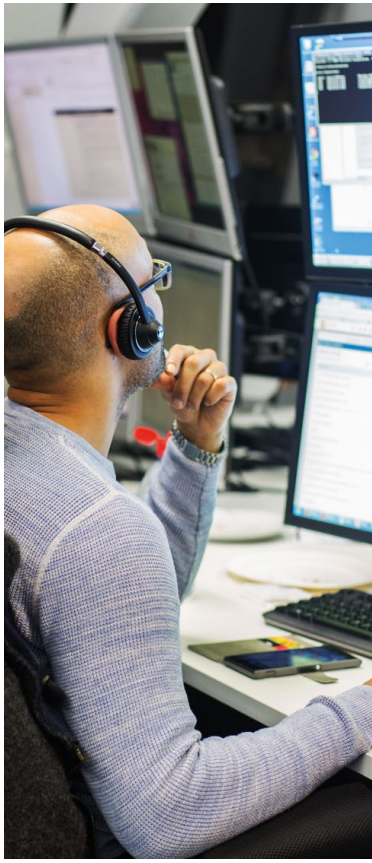
Michael Bateman
Director of Cyber Services
IT Lab

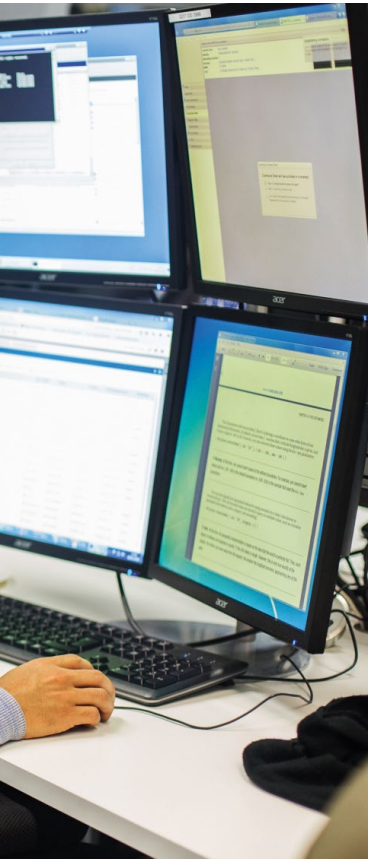
Security conscious organisations know that data protection demands a proactive approach. Many are either short on time or expertise, which presents a risk in itself. The GDPR places greater responsibilities on organisations to manage risk but this alone should not be the case for doing so.

Beyond the oft-quoted fines for GDPR infringements, any data loss is painful, impacting as it can on operations, service availability and staff time.

Often, the cost of a breach is heavier than the cost of sound security measures and monitoring.

Arguably, a price cannot be put on trust, reputation and stakeholder confidence. And in these turbulent times, there can be no better case for investment in this vital area.





THE LEGAL VIEW

Data privacy is now firmly on the boardroom agenda, as organisations reassess their activities under the light of the General Data Protection Regulation.

Mark Bailey
Partner
Charles Russell Speechlys

The GDPR is designed to improve the balance between private citizens, businesses and public authorities. Therefore conditions for processing, the rights of data subjects, the role of controllers and processors, consent and legitimate interest will become familiar C-suite lexicon.

Policies, privacy notices and third party contracts (notably with cloud providers) should be reviewed within the context of the GDPR, and based on a sound understanding of the new legislation.

As IT Lab rightly recognises, the GDPR demands the expertise of the IT, cyber security and legal professions. To achieve compliance, the disciplines are interdependent.

In the event of a data breach, board members should be cognisant of not just the potential for fines, but that all affected data subjects will be eligible for compensation, regardless of whether they are materially damaged by an infringement.

FREQUENTLY ASKED QUESTIONS

"Does this really apply to me and my company?"

Yes, if you handle or store personally identifiable data of any EU Citizens. This applies to Data Controllers (who determine the purposes, conditions and means of the processing of personal data) and Data Processors (who process data on behalf of the controller).

Personally identifiable data includes employees and B2B prospects/customers so don't assume you are immune from the GDPR if you don't sell to the public.

"Does Brexit mean that this doesn't apply to UK companies?"

No. The regulations apply to personally identifiable data belonging to EU citizens, regardless of where the company processing or controlling the data is located.

Furthermore, the regulations come into force on 25th May 2018 when the UK is likely to still be a member of the EU. Government announcements suggest that the UK will adopt EU regulations as part of domestic legislation.

"Do Data Processors and Data Controllers have the same obligations?"

Data Processors share the same obligations as Data Controllers, but face additional duties and liability for non-compliance, or acting outside of instructions provided by the controller.

Data Processor duties include:

- Processing data only as instructed
- Using appropriate technical and organisational measures to process personal data
- Deleting or returning data to the controller
- Securing permission to engage other processors

"What is personally identifiable data?"

Personally identifiable data includes information such as:

- Name
- Email address
- Social media posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

"I'll just pay the fine"

This is an approach that has been adopted by many businesses with respect to similar regulations and compliance regimes.

Unless the regulations or their enforcement changes from the current proposals, the fines will be significant – up to 4% of global turnover or €20 million (£16.9m), whichever is higher. The fines are intentionally high to discourage companies from taking this approach.

"I'll just get the lawyers to look at this"

Some of the current risks that a company faces, especially with respect to their supply chain, can be mitigated by contractual amendments.

IT Lab believe, however, that a large part of the work required to understand the risks is related to process and data architecture mapping and technology controls and procedures. Many of the risks can also be mitigated by adapting IT architecture and solutions.

IT LAB'S APPROACH TO GDPR ASSESSMENT, RISK MITIGATION & MANAGEMENT

DISCOVER

- Understand business process and context
- Identify data sources and consent
- Map data stores and personal data
- Data provided by third parties
- Discussion about contracts and relevant legal documents
- Map data management processes to understand how data is changed
- Understand control policy and process
- Understand technology architecture

ASSESS

- Assess compliance with GDPR obligations
- Data quality assessment
- Assess risk of non-compliance
- Assess contractual and commercial liability with customers and vendors
- Business case for mitigating non-compliance
- Highlight cyber security risks
- Grounds for processing
- Precedence of regulators
- Advice focused around mitigation of factors that could lead to fines
- Privacy impact assessment for new systems or developments to systems

CONTROL

- Propose new processes for data management
- Propose new technology solutions to enable better control of data
- Processes to improve consent management
- Processes to support deletion and portability of data
- Data retention
- Data Protection Officer
- New policies and procedures (including data retention and deletion policies and procedures
- Contract templates
- Data quality improvement and cleansing
- Implement solutions to mitigate cyber security risks
- Solutions for better protection of data
- Solutions for secure handling and migration of data
- Contract remediation
- Consent re-engineering
- Improved legal protection
- Improved processes

PROTECT

- Data quality improvement and cleansing
- Implement solutions to mitigate cyber security risks
- Solutions for better protection of data
- Solutions for secure handling and migration of data
- Contract remediation
- Consent re-engineering
- Improved legal protection
- Improved processes

REPORT

- Continuous data management and data quality management
- Pro-active security monitoring
- Reporting of ongoing consent management
- Reporting of data subject requests and compliance certification
- Submission of regulatory reporting
- Supply chain management

REVIEW

- Regular and continuous review
- Regulatory updates
- Data analysis
- Continuous compliance management
- Continuous risk reduction

BOOK A GDPR AUDIT

IT Lab's holistic approach to the General Data Protection Regulation ensures you've got it covered.

Our technology, risk management and data privacy experts work as one to help you achieve - and maintain - compliance with the GDPR.

To arrange an IT Lab GDPR Audit for your business, visit www.itlab.com/gdpr

Alternatively, call Jonathan Broadley or your account manager so we can discuss your requirements and provide a proposal for your audit.


0333 241 7689


hello@itlab.com


itlab.com/gdpr

itlab

London
2nd Floor
40 Bernard Street
Bloomsbury
London
WC1N 1LE

Manchester
Lowry Mill
Lees St
Swinton
Manchester
M27 6DB

www.itlab.com

©2018 IT Lab