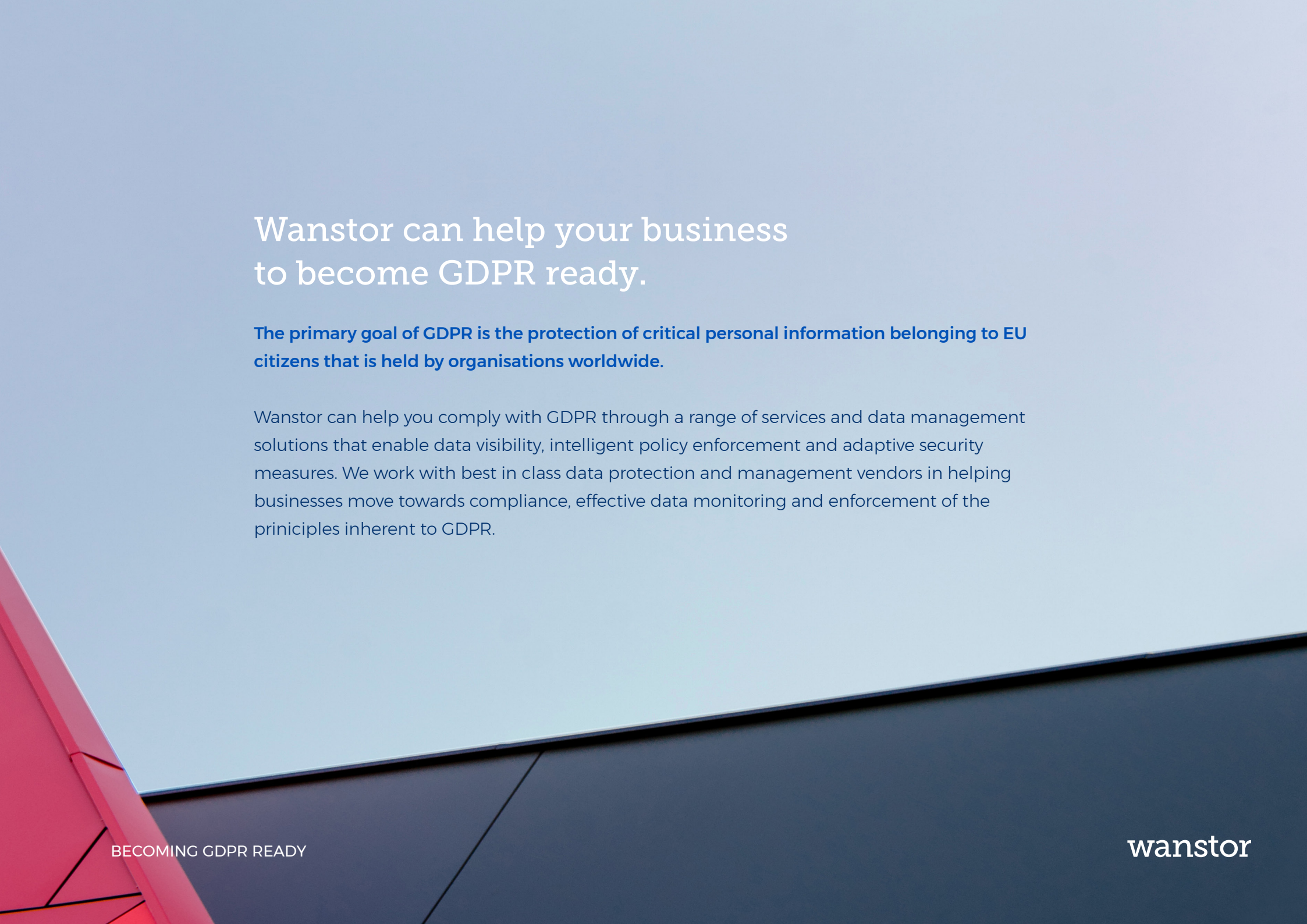
Putting the right IT & Technology Strategy in place for GDPR

wanstor

Wanstor can help your business to become GDPR ready.

The primary goal of GDPR is the protection of critical personal information belonging to EU citizens that is held by organisations worldwide.

Wanstor can help you comply with GDPR through a range of services and data management solutions that enable data visibility, intelligent policy enforcement and adaptive security measures. We work with best in class data protection and management vendors in helping businesses move towards compliance, effective data monitoring and enforcement of the priniciples inherent to GDPR.



Contents

+ INTRODUCTION

+ WHAT DOES GDPR MEAN FOR YOUR BUSINESS?

+ HOW DOES YOUR BUSINESS PREPARE FOR GDPR?

+ WANSTOR'S BEST PRACTICE APPROACH TO GDPR COMPLIANCE : A TIMELINE

+ WANSTOR CAN HELP YOUR BUSINESS TO BECOME GDPR READY

+ CONCLUSION

wanstor

The time is now

For some businesses, GDPR may still not have been actioned. With the EU expecting organisations to be fully compliant with the new regulations by May 2018, now is the time for IT departments to start planning. With GDPR on the horizon, they need to review data collection, security, management and governance models within the business.

The concept of GDPR is a simple one; the EU would like to implement a set of consistent data protection regulations across all member states, rather than having differing rules apply in different territories. Theoretically, this should simplify trading for most businesses - and it probably will do, once those organisations have undertaken programmes of work to ensure that they are GDPR compliant.

Unfortunately, in the short to medium term, businesses across the UK may experience some pain around data protection, management and governance whilst they put in place the people, processes and systems which will bring data governance into line with the new regulation after May 2018.

EU regulations as a whole are normally not particularly attention grabbing for IT departments; GDPR has, however, caught the eye of senior business executives and IT Directors, largely because of the substantial fines and impact on business that the regulations may have through failure to comply.

All organisations will want to ensure that they are compliant with data protection laws, and most UK businesses have a sound track record with regards to this. However, as GDPR will change the way that these organisations approach data strategy, this will force IT teams to analyse existing data collection, management and governance process so as to protect critical information without excessive cost and disruption to business operation.

This white paper will help to prepare for GDPR by providing a basic understanding of what is involved within different segments of the regulation, and how technology can be used to drive initial discovery in planning for May 2018 - as well as maintaining compliance into the future.

When Viviane Reding (EU Commissioner responsible for justice, fundamental rights and citizenship) unveiled her plans to overhaul data protection across the EU with the General Data Protection Regulation (GDPR), many businesses took little notice. Some business leaders thought the new regulations were too ambitious, unrealistic and time consuming to implement. Many business leaders thought because of concerns raised around these areas, the EU would dilute regulations which have been passed to make it easier. They were wrong.

But what should businesses focus on - and what does GDPR compliance look like? In the pages of this whitepaper, Wanstor offers a view on the primary issues within the regulation, how these proposals differ from current data protection laws, and what the practical compliance challenges are for your business.

> **With fines up to 4% of global annual turnover or 20 million Euros proposed, it shows how seriously EU regulators are treating the customers voice with this new regulation**

As the new GDPR regulation moves closer, the scale of this compliance challenge is starting to become a reality for many businesses. Organisations within the UK cannot afford to wait much longer with the penalties for non-compliance looming large. IT Departments need to start addressing data compliance today in readiness for these new regulations and to avoid costly fines and damage to reputation.

This new GDPR regulation is seen by EU parliament as a key element for Europe's Digital Single Market - the thinking being that if customers do not trust online services they may abandon these, forsaking the opportunities on offer. Customer confidence in online services represents the heart of new GDPR regulations. This means that levels set for compliance will be much higher than previous local data protection laws.

What does GDPR mean for your business?

Initially, new regulations can appear a serious challenge; you may not know where to start. Wanstor's data and information experts believe the major points from GDPR which businesses need to have under consideration as part of their GDPR compliance strategy are:

Geographic Range

The new GDPR regime will extend reach for current EU data legislation. In summary, there is no way to avoid this if your business operates within the EU or alongside businesses who are located within the EU.

There are of course already regulations and standards which span geographical boundaries - PCI DSS, for example - but these are specific, and mostly handled in a simplified manner (using a third party payment system).

GDPR proposes a far wider reach; if you are based in the United States and sell products or services to individuals in Europe, you will be subject to GDPR. Likewise, if you have a small business based in London and are trading with businesses across Europe, then you will be subject to GDPR.

Personal Data

The definition of personal data will broaden under new GDPR regulation, bringing far more information under regulation. This change is in keeping pace with an evolving digital environment - web 2.0, social applications - and rapid technological change (mobility, connectivity, social media, cloud) - both essential elements in achieving a 'Digital Single Market'.

Provision has also been made for the processing of data relating to national security, child protection, healthcare and research.

Supply Chain

With regulation coming in 2018, exposure to data-related liability will increase for customers, suppliers and partners - business deals negotiated now need steadfast preparation for new regulations. Parties need to document data responsibilities with clarity on increased data risk levels impacting on businesses negotiating with one another.

Reasons for Processing

The regulations that businesses will need to operate under whilst collecting and using data in future will prove considerably more rigid than at present. Businesses will be allowed to process only the minimal data necessary for performance of a contractual or legal obligation and for a limited time with explicit consent.

The rules around consent are expected to change with a clear indication of and acceptance around exactly what purpose personal data will be processed. No longer will assumed consent or reams of legalese unintelligible to the layman be acceptable.

EU member states may be allowed national legislation enhancing justifications in limited specific markets such as recruitment, but these will be exceptions to a rule.

Data Profiling

Under GDPR, data subjects will be able to contest decisions such as data profiling based on automated processes. There will be exceptions to this, such as where an automated process is necessary in allowing contractual performance or where it is required by law with safeguards protecting individual rights. The outcome of this requirement will require scrutiny and implementation by advertisers, insurers, recruiters and others in sectors relying on individual profiling as part of business activities.

Allowing and withdrawing consent

In protecting EU citizens, there exists the need for consent to use of personal information. This differs to current UK data protection laws - but there is an additional consideration under GDPR. Customers will be able to withdraw consent for use of their data. Withdrawing consent, or the **right to be forgotten**, will form a core tenet of GDPR. Data controllers will be required, in individual cases, to consider carefully competing rights to freedom of expression when considering requests for data removal or deletion. This may prove to be the most challenging aspect of GDPR for organisations; the tracking and updating of individual customer records coupled with a demonstrable ability to delete the same within 72 hours.

Additionally, businesses must ensure that information shared with third parties is also similarly maintained.

International Transfers

While GDPR builds on current data protection frameworks with respect to general principles for international transfers, rules have been extended to apply to processors and to onward transfers of personal data to third countries or international businesses.

This suggests that businesses will need greater understanding of companies and individuals with whom they transact, and ensure that they maintain accurate records of transactional information.

Security & Breach Notification

Under GDPR, data breach notifications to relevant data protection authorities where a breach causes individual risk will be a requirement. This is an area where demonstrable management by businesses will become essential. Strict timelines and details have been established requiring the notification of both authorities and individuals affected within 72 hours of any data breach.

Breach notifications must include the nature of the breach, the identity of attackers or responsible parties, recommended measures on preventing adverse effects, and how the business will address said breach. The requirement for appropriate security will extend to both data processors and controllers, and will include demonstration of compliance with applicable codes of conduct, including:

+ The ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data

+ Processes for regularly assessing, testing and evaluating effectiveness of technical and organisational measures around security of data processing

+ The ability to restore availability of and access to data promptly in the event of a physical or virtual incident

+ The pseudoanonymisation and encryption of personal data

Businesses should note that GDPR is not simply a guideline to process and best practice; it represents a regulation that indicates appropriate and reasonable technical measures to be implemented when enforcing data policies and compliance.

Data Protection Officers

In pursuit of GDPR compliance, a new position will be required within the organisational structure: that of Data Protection Officer. This role functions primarily to monitor internally for compliance with GDPR, ensuring appropriate protection of any information held. The regulations around appointment of a Data Protection Officer are reasonably complex - in many cases, this function will be outsourced to specialist organisations able to advise on best practice and ensure that relevant processes are in place.

The Data Protection Officer should make objective analysis of existing records and develop plans to ensure that all data - both past and present - is GDPR compliant. Wanstor believes that appointment of a Data Protection Officer should be the first step before undertaking a GDPR strategy, owing to background work required. Securing this position will enable a business to manage GDPR from one location within the organisation, meaning centralised accountability - not compliance requirements being managed by disparate departments.

Fines & Enforcement

The final concern for any organisation will be the headline grabbing penalties that are to come associated with GDPR.

With fines of up to 4% of global annual turnover, or €20 million - whichever proves higher - GDPR puts data protection on a par with anti-trust and anti-bribery laws.

No longer can businesses give occasional or vague consideration to compliance with data protection; they will instead need a data protection strategy in place to monitor and manage the protection of personal information.

Privacy

Data controllers will be required to implement appropriate and relevant technical, business and organisational processes in ensuring that data processing safeguards and the rights of data subjects are paramount at all times. Only the necessary minimum of personal data may be processed and may not be disclosed more widely than is absolutely necessary.

The information directly above has led to an inordinate amount of hype around privacy by design. At Wanstor, we believe this is not unjustified, but that businesses should remain focused on delivering practical data strategy outcomes covering privacy.

IT departments must realise that privacy by design will mean technology requires deployment and management, and should look to deploy solutions capable of monitoring and managing the transit of information within organisations. Breaches and information barred from transit must be included in application reporting, along with any and all means by which that information may be extracted.

Data Visibility

The first step in becoming GDPR compliant is to understand where your data is held and its visibility within your business. Wanstor can help you discover where customer's personal data is distributed amongst your servers, desktops, notebooks and network shares. We can also help to inspect information before it leaves your business via email, social media, cloud storage and collaboration apps, in ensuring that it follows GDPR guidelines.

Giving this level of visibility to your data can be considered part of a privacy audit, an assessment of control currently exercised over your information or, at some point in the future, as part of a Data Protection Impact Assessment. It can also be used to form part of a **right to be forgotten** request, where discovery of any information held in unstructured files on endpoints and file servers is required. Deletion can then be carried out either manually or automatically.

Agile Security Management

Protecting your data outlet points is critical in ensuring that information to be regulated under GDPR remains safe from loss or leaks through accidental mistakes, malicious insiders or external attacks. Having an agile IT security management process applied in real-time based on specific GDPR policies can prevent such occurrences.

Whether your business requires automated redaction, encryption, blocking, moving or deletion of information, Wanstor can implement an agile information security management strategy which automatically enforces GDPR regulation. This means that your business remains protected, you retain customer trust, and that you ensure end users are utilising data for the right purpose.

Data Policy Implementation

At Wanstor, we understand that not all data, access and sharing rights are created equal. Intelligent data protection policies must be applied consistently across all channels, and be based on GDPR regulation. Intelligent data policy implementation and management utilises both content and context in policy decisions; context being the sender, recipient, and communication mechanism (such as email, web or endpoint). A single shared policy creates consistency, along with ease of deployment and use. A document sent via corporate email may be encrypted based on policy action.

The same file may be uploaded to a cloud collaboration site, in which case policy action would involve redacting sensitive information. Finally, the same file may be transferred to portable USB - at which point, policy action will block it. Wanstor can help you to implement and manage a range of policies, balancing business needs and customer trust.

Data Governance

Whether you are IT Manager, Data Protection Officer or Head of Legal, you will need complete visibility of reports, policy violations, quarantined data, logs and more as part of GDPR. Wanstor's track record in managing large data volumes and retrieving historical data make us an ideal partner in developing real-time GDPR policy rules and adaptive security enforcement measures. We have extensive experience in implementing violation and breach analysis for identification of personal data loss, sources and exposure required for notifications.

Additionally, we can provide granular tracking of information at a file and a sub-file information level in monitoring information across the business edge to both suppliers and partners. We can provide source reports to determine which information has been sent and to where, allowing identification of relevant parties in the event of specific **right to be forgotten** requests being made.

How does your business prepare for GDPR?

How will GDPR work in practice? Without the regulation in place, it is difficult to know what GDPR really means for businesses. Wanstor believes that for most, it will approximate one of the following two examples.

Example One

A multinational company with several businesses in EU Member States maintains a social media service collecting information and image content from customers

Under current legislation: With data protection safeguards varying substantially between Member States, this service fell foul of data protection laws by retaining both customer image data and personal information. To address this violation and maintain the service, the organisation offered additional guarantees and safeguards to residents after negotiation with the DPA. The business did, however, refuse to offer the same guarantees to individuals in other EU Member States. Data controllers currently operating across borders must often comply with different (and often contradictory) obligations.

Under GDPR: A single, pan-European law for data protection will exist, replacing current national laws. Business worldwide must apply EU data protection law when offering services in the Union.

Example Two

A small publishing company is expanding business activities from France to Spain

Under current legislation: The company's data processing activities would be subject to a different set of regulations within Spain, and the company would have to deal with a new regulator. The costs of obtaining legal advice and adjusting the business model in order to access this new market may prove prohibitive - some member states do, for example, charge notification fees for processing data.

Under GDPR: The new data protection regulation will scrap all separate notification obligations and costs associated therewith, to be replaced by a single unified notification along with consent and erasure processes to be followed. The aim of this new data protection regulation is the removal of any obstacles to cross-border trade.

Wanstor's Best Practice Approach to GDPR Compliance : A Timeline

Immediate

Assessment

Initial GDPR Assessment & Workshop covering People, Processes, Data, Governance, Security & Privacy

GDPR Business & IT Roadmap to plan action required in becoming GDPR compliant

Customer Data Identification to identify customer data storage location & management

Before May 2018

Design

IT Design for GDPR covering Governance, Staff Training, Recruitment, Communication & Process Standards

Design of IT Services and Solutions covering Privacy, Data Management & Security Management standards

Transformation

Develop & Embed GDPR procedures, processes, & tools

Deliver GDPR training for staff across the business

Develop & Implement Standards for Privacy by Design, Security by Design & Data Management Policies

May 2018

After May 2018

Operations

Execute all relevant business processes relating to GDPR

Monitor & Manage Security & Privacy

Manage Data subject access & consent rights across all data centres & operating systems

In-Life Management

Improvement by Monitoring, assessing, auditing, reporting & evaluating business adherence to GDPR standards

Outcome

Identification of impact on IT & Business

Technical Assessments

Generation of GDPR readiness roadmap

Outcome

Defined implementation plan covering Data Protection controls, processes & solutions

Processes & process enhancements complete

Customer Data Discovery completed & assessed

Data classifications & Data Protection Governance Model in place

Outcome

GDPR operational framework in place

GDPR-compliant business operation commences

Execution of GDPR strategy monitored

Stakeholders issued proof of Compliance

Continual Service Improvement plan for GDPR implemented

Conclusion

GDPR arrives on 25th May this year - your business should already have started planning for the impact. IT teams will be taking the lead at this stage in pursuing compliance, viewing the regulation as an opportunity to formalise information management and data governance. For some, this may provide first sight of digital information held on customers, suppliers, partners and employees - a huge opportunity for business to derive value from data management strategies and empower itself for the future.

We believe the process of data compliance begins with understanding data, building appropriate corporate policies around protection, and then enforcing those policies with technology. The GDPR affects any organisation, in any sector, that does business within the EU.

Wanstor provides data solutions that will help you to become GDPR compliant - from initial assessment through to in-life data management, Wanstor can help your business at each and every stage of the GDPR compliance lifecycle.

+ + +

Wanstor | 124-126 Borough High Street | London | SE1 1LB |

info@wanstor.com

wanstor