insITe BUSINESS SOLUTIONS

(616) 421 - 8325
trustedinsite.com
tellmemore@trustedinsite.com

Expert Help with **GDPR Compliance**, Risk Assessment, and Strategy

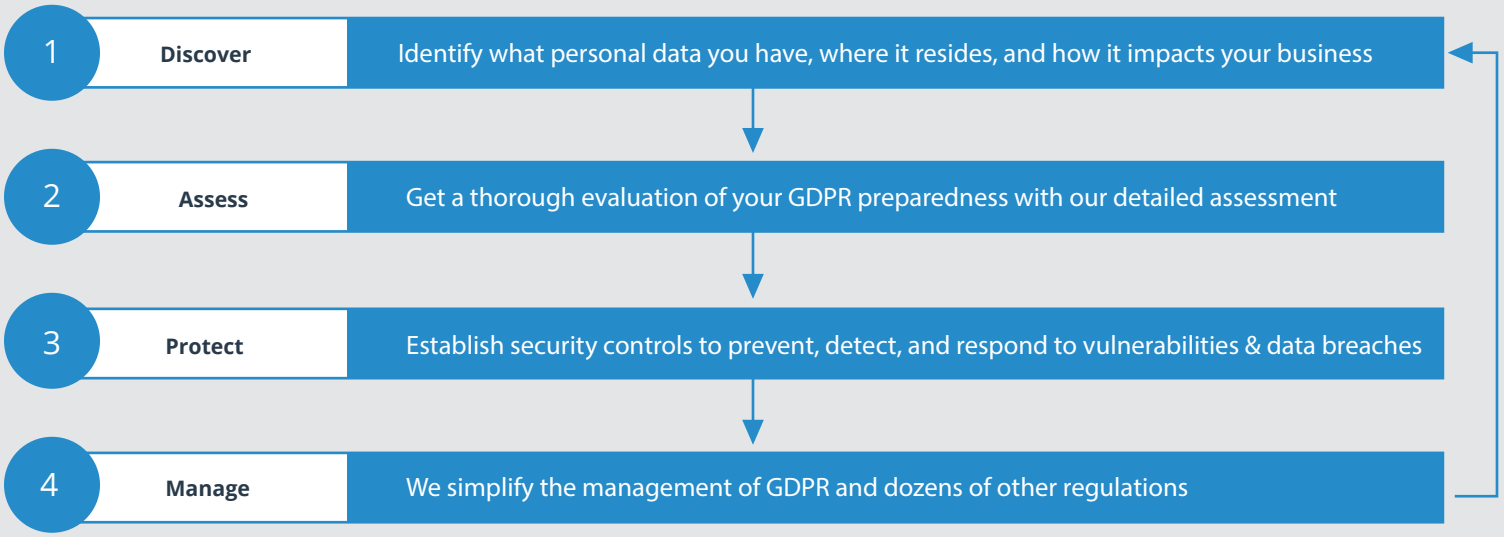
The GDPR sets new standards for privacy and personal data, and it's not just Europe

In May 2018, a new European Union (EU) privacy regulation goes into effect with broad reaching implications for organizations around the world. The regulation, called the General Data Protection Regulation (GDPR), introduces new requirements on privacy, security, and compliance, accompanied by appropriate security measures.

- ☑ Enhanced personal privacy rights with more flexible controls for individuals
- ☑ Increased duty for protecting data including stricter guidelines
- ☑ Mandatory breach reporting, privacy personnel training, and DPO officer
- ☑ Significant penalties for non-compliance

GDPR: Not just Europe

The GDPR applies more broadly than many people think. The law imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in EU or that collect and analyze data tied to EU residents — no matter where they are in the world. GDPR is applicable to organizations of all sizes and all industries and personal data can be found in many places like email content and photos.



InsITe Can Help

We have the skilled personnel, process knowledge, and technology expertise to evaluate your GDPR readiness and help you on your path to become, and stay, compliant. An ideal starting point is a detailed assessment of your GDPR readiness. We offer this as a complementary service. We'll work with you to evaluate your organization's privacy posture, uncover risks, provide expert guidance around the GDPR, and offer recommendations specific to your organization.

Key changes required by the GDPR

Personal Privacy
Individuals can now:

- Object to processing of their personal data
- Correct errors in their personal data
- Access their personal data
- Erase their personal data
- Export personal data

Control & Notify
Organizations need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies
Organizations need to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT & Training
Organizations need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

How InsITe approaches GDPR compliance

Assess and Manage Risk: An on-going assessment of your compliance posture with actionable insights to improve your data protection capabilities.

Protect Personal Data: Protect data with industry leading encryption and security technology that's always up-to-date and assessed by experts.

Streamline Processes: Centralize processing in a single system, simplifying data management, and audit-ready tools that help you collaborate between teams and manage your processes.

We'll work with you to uncover risk, and take action

Discover and catalog data sources, increase visibility with auditing capabilities, and identify where personal info resides across devices, apps, and platforms

Enforce use policies and access controls across your systems, classify data for simplified compliance, and respond to data requests and transparency requirements

Protect user credentials with risk-based conditional access, safeguard data with built-in encryption technologies, and rapidly respond to intrusions with built-in controls to detect and respond to breaches

GDPR Solutions with InsITe

We will make the complex world of security simple, and our audit and solution will be custom tailored to your business. We employ our **ESIM (Evaluate, Strategize, Integrate, Maximize Results)** process in every project we take on. ESIM is the secret ingredient in all we do, and this mindset makes sure we **understand the problem before we strategize to find the best solution.** It is a structured approach to your needs and allows us to find the very best solutions for your business, long term.

www.trustedinsite.com | (616) 421 - 8325 | tellmemore@trustedinsite.com

How does GDPR impact your business?

1. Does the GDPR apply to my organization?

- GDPR Impacts organizations that offer goods and services to people in EU or collect and analyze data tied to EU residents, no matter where they are
- Includes companies, government agencies, non-profits, and others
- For all sizes of organizations: small, large, and enterprise

Pro Tip:

The GDPR isn't just Europe – it applies more broadly than many people think.

2. Is the data my organization processes subject to the GDPR?

- GDPR regulates collection, storage, use, and sharing of "personal data"
- Includes any data related to an identified or identifiable person
- Personal Identifiable Information (PII)
- Some identifiers: IP address, employee information, sales data, customer data, and biometric data

Pro Tip:

The GDPR is all about personal data, which can reside in: customer databases, feedback forms filled out by customers, email content, photos, CCTV footage, loyalty program records, HR databases, and more.

3. What are the risks if we don't comply?

- Fines can be up to 4% of annual turnover or €20 million
- Individuals (or organizations acting on their behalf) can start civil litigation
- Other organizations may only work with you if you're compliant

Pro Tip:

Up until now, data protection laws did not include significant fines. The GDPR changes things dramatically. GDPR compliance is not a one-time activity and carries significant penalties for non-compliance.

4. What are the main requirements?

- Transparency, fairness, lawfulness when handling and using personal data
- Data processing minimization
- Collection and storage minimization
- Ensure accuracy of personal data

Pro Tip:

Organizations need to be clear how they handle personal data– there must be a lawful basis. Processing is limited to specified, explicit, legitimate purposes. Storage should be adequate for the intended purpose.

5. What does transparency really mean?

- Organizations must tell individuals about their data processing
- Why it is processed, how long it is stored, with whom it is shared, and is it transferred outside the EU
- Easy to access and understand format

Pro Tip:

Data controllers must ensure that anyone whose data is collected is kept adequately and sufficiently informed about just what is being done, and will be done, with their data.