The Race to GDPR Compliance

{e}mazzanti technologies®

Quick Facts

- Founded in 2001, over 18 years of customer success
- Average accelerated revenue growth 20% each year
- 2018 Acquisition of Messaging Architects
- 2017 Acquisition of ForceWorks Microsoft Partner of the Year in Dynamics
- 2016 Acquisition of Liqui-Site, award-winning Digital Marketing Agency dedicated to Custom Websites, Brand Development, Mobile Services and more
- 2015 Acquisition Cloud Services Team dedicated to Azure Services & implementation
- Nine consecutive years on Inc. 5000's list for fastest growing privately held companies
- WatchGuard 5x Partner of the Year, First International Platinum Partner
- NJBIZ 2017 New Jersey Business of the Year
- Microsoft Partner of the Year: 2015, 2013, 2012
- Microsoft Top 200 Worldwide VAR
- Microsoft GOLD Partner
- Member of PCI Security Standards Council
- QIR and CISSP Certified Employees

Support

International Support in Multiple Languages

Spanish, Italian, French, Albanian, Sri Lankan

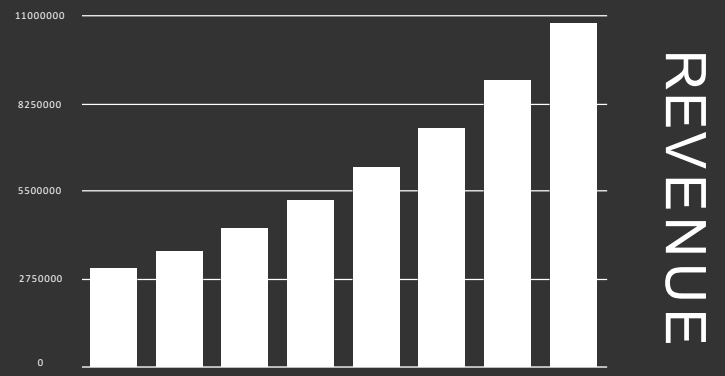
Support Available 24/7 x 365

Offices on the East and West Coast

Global offices in Europe, Middle East & Asia

Certified Engineers & Developers to perform Network Services, Cloud Support, and Digital Marketing

Performance



2015|2013|2012 Microsoft Partner of the Year

WatchGuard 5x WatchGuard Partner of the Year

Inc. 5000 | 5000

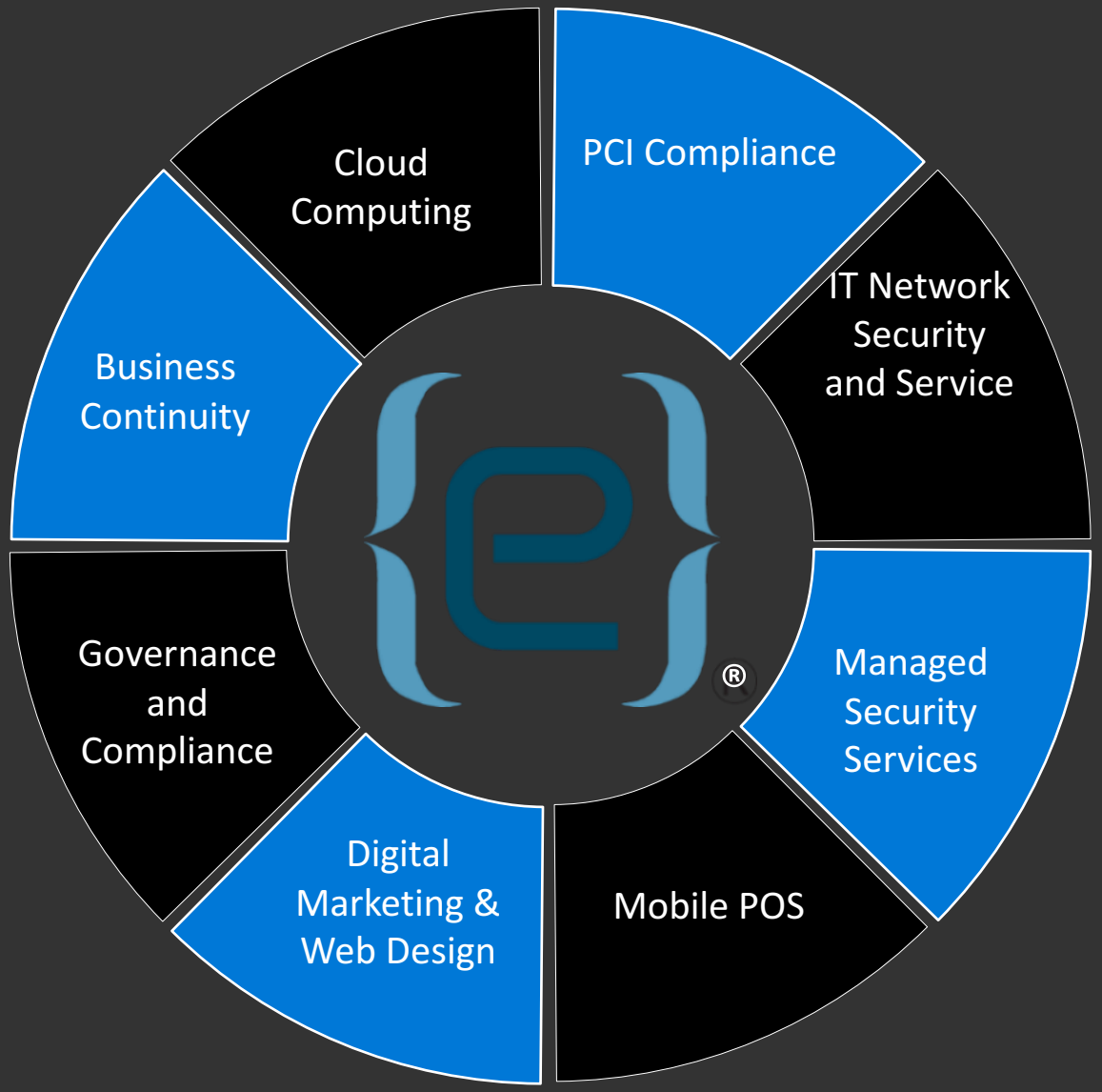
2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010

mazzanti technologies

Our Services

- IT Network Security and Service
- Managed Security Services
- Cloud Computing
- Business Continuity and Disaster Recovery
- Corporate Governance and Compliance
- Email Hosting, Filtering and Anti-virus Protection
- Digital Marketing
- Secure Mobile Workforce Solutions
- POS Implementation & Maintenance
- Managed Print Services
- Website Design & Hosting
- Store Relocation Services
- Outsourced IT

Competencies



Our Speaker

Carl Mazzanti

President & Cofounder at eMazzanti Technologies

Founded in August, 2001, and built with a business continuity mindset, Carl's firm, eMazzanti Technologies, has done everything possible to recover and keep his customers open when the worst happens. Within 72 hours of Sandy's devastating landfall, 100% of his 300+ customers were back up and running.

Carl Mazzanti lives by innovation and continuous learning, seeks only long-term customers, and systematically tracks customer satisfaction. After consulting with thousands of businesses, Carl has accumulated extraordinary first-hand knowledge of the numerous methods and tools small businesses can employ to reduce costs and increase their productivity and revenue.

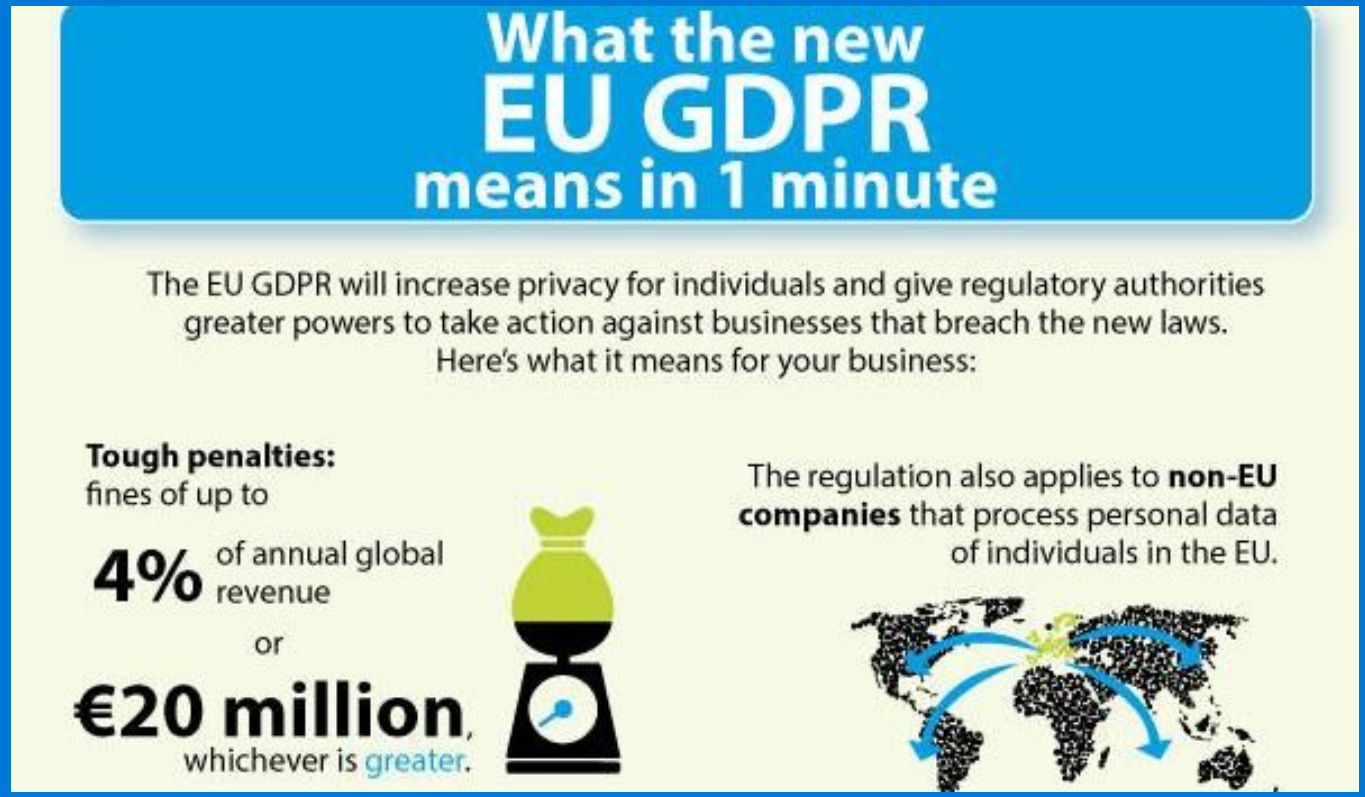
Carl is a graduate of Georgetown University, with a triple major in Finance, New and Small Business Management, and International Business. Jennifer, his wife and business partner, is co-founder and a key player in the business. His interests include outings with his two boys, snowboarding, sailing, and minor league baseball.

Contact Details:

GDPR@emazzanti.net

844-360-4400

What is GDPR?



The European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016, replacing an outdated data protection directive from 1995. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU.

The provisions are consistent across all 28 EU member states, which means that companies have just one standard to meet within the EU. However, that standard is quite high and will require most companies to make a large investment to meet and to administer.

Key Changes Under GDPR

Personal Privacy, individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- **Erase their personal data (EX: reply that data is deleted and then email is received by customer from a different platform or list)**
- Object to processing of their personal data
- **Export personal data (EX: form emails that leave the EU for processing)**

Key Changes Under GDPR

Controls and Notifications and Transparent Policies, organizations will need to:

- Protect personal data using appropriate security
- **Notify authorities of personal data breaches (EX: Where and do you know how)**
- Obtain appropriate consents for processing data
- Keep records detailing data processing
- Provide clear notice of data collection
- Outline processing purposes and use cases
- **Define data retention and deletion policies (EX: Distributed data across cloud applications)**

Key Changes Under GDPR

IT and Training, organizations will need to:

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

How Will it Affect My Business?

Which companies does GDPR affect?

Any company that stores or processes personal information about EU citizens within EU states **must comply** with the GDPR, even if they do not have a business presence within the EU.

Specific criteria for companies required to comply are:

- **Processes personal data of European residents** with a presence in an EU country or not.
- **Fewer than 250 employees** where data-processing impacts the rights and freedoms of data subjects or includes certain types of sensitive personal data.

This law effectively addresses all companies. Surveys showed that 92% of U.S. companies consider GDPR a top data protection priority.

How Does this Affect Me?

But what does GDPR mean for individuals? **You have the power to hold companies accountable like never before. Data Protection Authorities (DPAs) will have the power to enforce much more severe penalties for breaches of personal data.**

The definition of 'personal data' has widened and now explicitly includes online identifiers such as IP addresses and mobile device identity. Organizations will need to attain explicit consent from individuals regarding the processing of their data, and companies will no longer be able to use long, illegible terms and conditions. Individuals will also have more rights regarding the processing of their data, for example relating to data erasure (often referred to as the 'right to be forgotten') and data portability, which is the right to transmit their data to another controller. The reporting of personal data breaches will become mandatory. **Under Article 33 of the GDPR, organizations must report breaches of personal data to the DPA within 72 hours of becoming aware of them.**

The Right to be Forgotten

Risks of Not Being Compliant

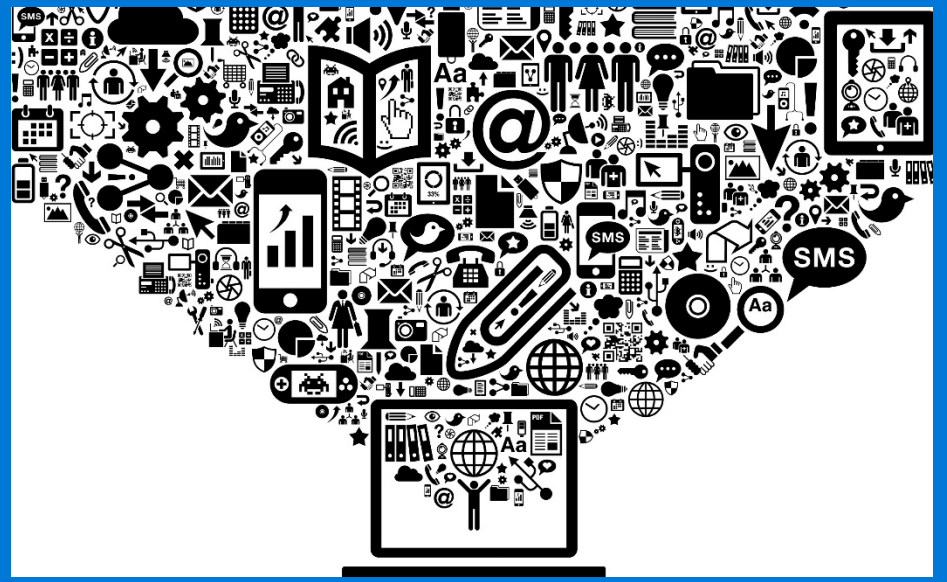
Tiered Penalty Structure

Violations of basic principles of the GDPR can result in **fines of up to four percent of annual global revenue**. While such a fine could prove devastating, particularly to a small business, there are actually two tiers of penalties. In addition, fines represent just one of several possible sanctions.

Once imposed, fines fall into one of **two tiers**:

- Lower Tier – In general, these involve failing to adequately integrate data protection by design into business operations. Fines can be imposed of up to **10 million euros or two percent** of the organization's annual global revenue, **whichever is greater**.
- Higher Tier – These involve more serious infringements on an individual's privacy rights and freedoms. Fines in this category can reach as high as **20 million euros or four percent of annual global revenue**.

Unstructured Data & You

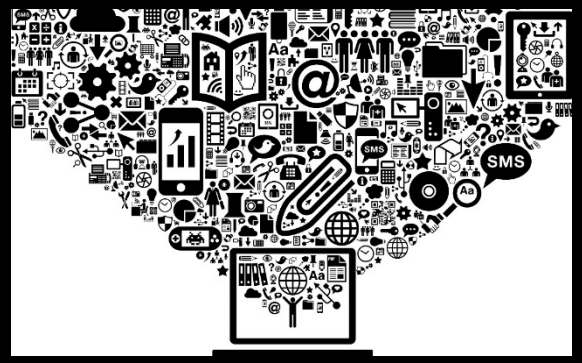


Unstructured data is often stored in 100’s of different formats.

Stored in hard-to-reach systems like:

- Microsoft Exchange
- Office365
- SharePoint
- Skype
- OneDrive
- zip-files
- local folders on the employee's laptop
- etc.

Unstructured Data & You



What should you do?

1. Define rules about what constitutes PII in your organization, e.g. social security numbers (SSN), address information, diagnosis, religious beliefs, life events, race, gender, etc.
2. **Identify** islands of **unstructured data**
3. **Regularly index and flag data** that contains probable PII or other sensitive data
4. Empower your organization to stay compliant. **Enable the owners of data** to review flagged data items and decide to keep, move, delete, encrypt, etc.
5. Produce overview dashboard to department heads, general management and DPO about the state of GDPR compliance for unstructured data
6. **Hire a Professional or Firm to navigate this business need.**

Risks of Not Being Compliant

Additional Consequences of GDPR Non-Compliance

Although severe fines gain the most attention, other consequences of GDPR non-compliance can prove incredibly harmful to your business without it directly hitting your wallet.

- **Damage to Reputation**: When consumers learn that your organization has had an incident, they will be wary about trusting you with their data. Even a formal reprimand can result in loss of market share and reduced consumer confidence.
- **Cost of Damage Control**: Once an incident has occurred, it will be costly to conduct investigations and implement remediation measures.
- **Withdrawal of Certification**: Supervisory authorities can mandate withdrawal of a certification.
- **Ban on Processing**: Supervisory authorities may also order a temporary or definitive ban to keep your organization from processing personal data.
- **Liability for Damages**: According to Article 82 of the GDPR, an individual who has suffered material or non-material damage as a result of an infringement of the GDPR can claim compensation from both data controllers and data processors.

Benefits of GDPR Compliance

Enhance Your Cybersecurity

There is no company in the world that can afford to take the risk of cybersecurity ignorance, given the costs of data breaches and business downtime caused by theft or loss of critical data.

The legislation requires organizations to **identify their security strategy and adopt adequate administrative and technical measures** to protect EU citizens' personal data.

In fact, the regulation encourages you to reevaluate and improve your overall cybersecurity strategy: You will have to establish thorough control over the entire IT infrastructure, build healthier data protection workflows and streamline security monitoring.

Benefits of GDPR Compliance

Improve Data Management

To be compliant, you should know precisely what sensitive information you hold on people.

Obviously, the first thing you want to do for your GDPR compliance is to audit all the data you have.

With the findings of an audit, **eliminate the redundant, obsolete and trivial (ROT)** files that your organization retains, though they don't have business value.

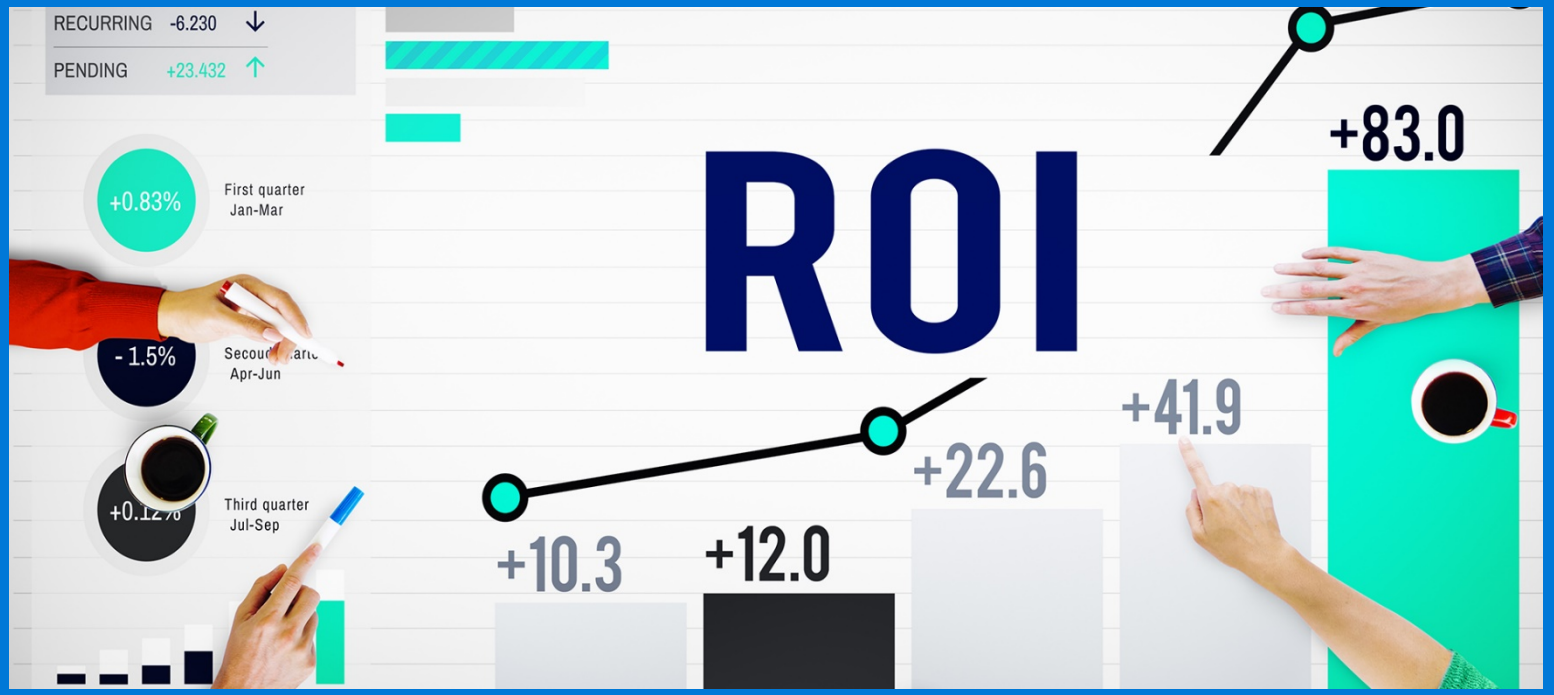
Next, implement mechanisms for fulfilling another GDPR requirement -- **make data globally searchable and indexed.** This will help you more easily handle subjects' requests to delete the data if they exercise their right to be forgotten.

Benefits of GDPR Compliance

Boost Audience Loyalty And Trust

GDPR compliance can support your business in helping you build more trusting relationships with your customers and the public generally. Since consumers are becoming more and more suspicious about how their data is handled, the transparency and responsibility you demonstrate will encourage trust in your brand. Thus, you can use the GDPR to underline that you do care about the privacy of your current and prospective customers and stand head and shoulders above your competitors.

Benefits of GDPR Compliance



Increase Marketing Return On Investment (ROI)

One of the key principles of the GDPR is that the organization should implement an opt-in policy and have a data subject's consent to process their personal data. With this information at hand, you will be able to experiment with niche marketing by tailoring your message to the specific needs and habits of a clearly defined audience that has more interest in your brand. Such a granular marketing approach will result in higher click-through, conversion rates and social sharing, and increase your marketing ROI as budgets and efforts will be spent wisely.

Navigating GDPR Compliance – Website Tips

Regardless of our attitudes about new regulations and perhaps some wishful thinking, the GDPR rules intended to strengthen data protection and privacy within the European Union (EU) will affect all but the smallest companies in the U.S. Those most impacted are organizations that provide products or services to individual customers, including retailers, financial services, insurance and legal services and others.

Here are some ways that you can get your website compliant with the new GDPR rules:

- **Online Contact Forms**
- **Privacy Policy**
- **Email Marketing**
- **Handling Data**

DPIA – Data Privacy Impact Assessments

The DPIA is one of the specific processes mandated by GDPR. Organizations must carry out a DPIA where a planned or existing processing operation –"is likely to result in a high risk to the rights and freedoms of individuals".

Identify the need for the DPIA – determine whether the inherent risks of the processing operation require you to undertake a DPIA.

Describe the information flow – be able to describe how the information within the processing operation is collected, stored, used and deleted.

Identify privacy and related risks – catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data you collect and/or process.

Identify and evaluate privacy solutions – for each identified risk to the personal data, make a 'risk decision', i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.

Sign off and record the DPIA outcomes – record the outcomes of the DPIA (steps 1-4) in a report that is signed off by whoever is responsible for those decisions. Where a high risk has been identified, the organization must submit the DPIA to the regulatory authority for consultation.

Integrate the DPIA outcomes into the project plan – you will need to continually refer to the DPIA in order to ensure that it is being followed and that its responses to the risks have been implemented effectively.

How We Can Help

The advent of the GDPR demands that organizations devote sufficient resources to risk management and compliance. And in particular to information technology. So how can technology help organizations accelerate their response to the legislation and become GDPR compliant?

Data management and discovery

The initial step is to discover personal data across your organization and protect it from unauthorized access. By identifying and controlling personal data—at rest, in motion, and in use—organizations will be uniquely positioned to enforce the GDPR compliance.

Identity and access governance

Organizations need to centralize and govern user identity and manage access, especially in the case of privileged users. By automating this user management, organizations benefit from 'who has access to what' insights, higher user productivity and GDPR compliance.

Privileged access management and threat analytics

Under the terms of the GDPR, data controllers must report any data breach within 72 hours of the incident occurring. By managing privileged access, organizations can more easily protect privileged activities and enforce data breach detection and notification.

Test data management and synthetic data generation

Test data management (TDM) is the process of providing, distributing, and managing test data for development teams—and TDM takes on more urgency as the GDPR deadline looms. Robust and efficient TDM practices are key to overcoming compliance hurdles and avoiding the penalties associated with the GDPR. By using synthetic data, organizations will avoid the pitfalls associated with masking production data.

API management

API management is the foundation for a future-proof GDPR-compliant architecture. It enables organizations to quickly and easily adopt rules for gathering consent, and inform users about the regulations relating to data access and data portability.

Are You Ready?

GDPR Readiness Assessment

- Does your organization have sufficient technical measures and processes in place to secure personal and sensitive data?
- Are your data collection, data processing, and supporting technologies built to include privacy and protection principles?
- How much of your personal and sensitive data is currently encrypted both at rest and in transit?
- I would describe my organization's process for classifying and labeling end user sensitive data as: 100% automated, partially automated, Manual, Don't know/not sure
- Which of the following protection policies do you use to classify and label sensitive data?
  - Encryption
  - Rights restrictions
  - Visual markings (e.g., watermarks)
  - Restricted access
  - End-user notifications
  - None

If you are not sure about how your organization stacks up in these areas, you are not alone. The good news is that there are plenty of additional resources to broaden your understanding of GDPR compliance, help you get ready for GDPR, identify issues you may not have considered and learn how to accelerate your compliance journey.

Thank You!

844-360-4400

GDPR@emazzanti.net