How Businesses Can Stay GDPR Compliant With Data Discovery

Table of Contents

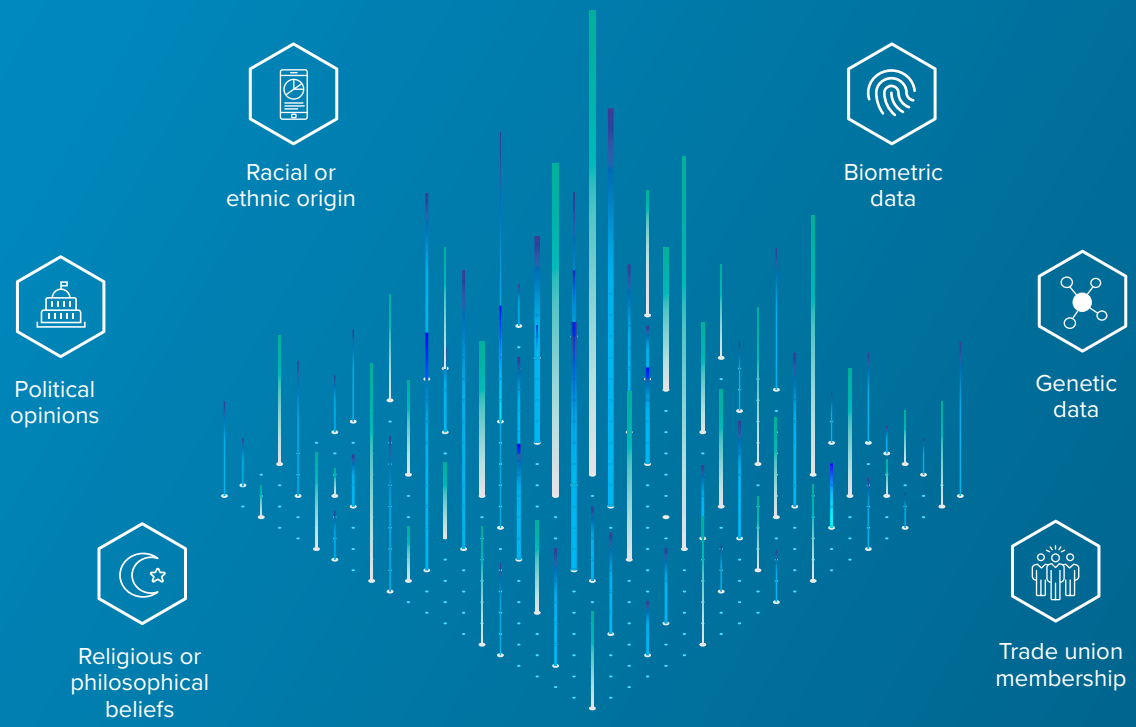
SECTION 1

What is GDPR?

The General Data Protection Regulation (GDPR) is the European Union's (EU) data privacy and security law. The EU put GDPR into effect on May 25, 2018. The law was designed to give European citizens and residents more control over how their personal data is collected, used, and protected online.

GDPR applies to any organization (large or small) that handles data belonging to EU citizens and residents, regardless of where the organization is located.[1] Under GDPR, a personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.[2]

GDPR considers the following to be sensitive data:



Under GDPR, organizations can only legally process sensitive data if they satisfy at least one of the following conditions:[3]

- Explicit consent of data subjects
- Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement
- Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Data manifestly made public by the data subject
- Necessary for the establishment, exercise, or defense of legal claims or where courts are acting in their judicial capacity
- Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures
- Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

SECTION 2

Differences Between EU & Australian GDPR

In contrast to the EU's GDPR, many people are unaware that Australia also has its own privacy law. This law is sometimes referred to as the "Australian GDPR," but is formally called The Privacy Act 1988. This Australian Privacy Act was originally introduced in late 1988 and has since undergone over 80 revisions that incorporate various updates and amendments.

Australian GDPR requires companies to adhere to the following privacy principles:

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information
- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Adoption, use or disclosure of government related identifiers
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

Under the Privacy Act, Australian organizations' and their coinciding privacy policies must address:

- The type of personal information being gathered and stored
- How it is found and stored
- Why the information is kept and used
- How individuals can exercise their rights with their personal information
- How to file a complaint about a company's handling of an individual's PII
- Information about overseas relocation of personal information

Like the EU's GDPR, Australian GDPR requires companies to keep data safeguarded and to securely erase PII when necessary. Additionally, under both laws, data breaches are expected to be reported to authorities as soon as possible. Both laws also require companies to report data breaches to individuals if the event is severe enough.

SECTION 3

Consequences of Noncompliance

Direct Financial Consequences

Companies that violate GDPR can incur high fines. A recent Gartner report found that two years after GDPR was initially implemented, Europe's major privacy regulators have acclimated to the volume of GDPR-related complaints.[4] This is a key shift because it means regulators are moving beyond reactive enforcement (driven by complaints) to proactively seeking out instances of noncompliance.

There are two tiers of GDPR fines:[5]

Less severe infringements:

- *Violations of the articles that govern*:
  - Controllers and processors (Articles 8, 11, 25-39, 42, and 43)
  - Certification bodies (Articles 42 and 43)
  - Monitoring bodies (Article 41)
- *Fines associated with these infringements*:
  - Up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher

More severe infringements:

- *Violations of the articles that govern*:
  - The basic principles for processing (Articles 5, 6 and 9)
  - The conditions for consent (Article 7)
  - The data subjects' rights (Articles 12-22)
  - The transfer of data to an international organization or a recipient in a third country (Articles 44-49)
- *Fines associated with these infringements*:
  - Up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher

No company is immune to these fines; there have been many high-profile GDPR cases. For example, in late 2020, Twitter was fined around $550,000 for failing to document and declare a data breach in accordance with GDPR regulations.[6]

Customer Trust

The consequences of a data breach extend beyond the direct fines as well — loss of customer trust and lost business are also significant repercussions. A GDPR fine in itself might seem small and be manageable for an organization, but losing your customers' trust can have a devastating impact on your brand and shareholder value. In 2020, the average cost due to business loss from a data breach was $1.52 million — an amount that can have a significant impact on a company's bottom line.[7]

SECTION 4

Common Compliance Challenges

Although GDPR regulations have been in place for close to three years, many companies are still facing challenges when trying to maintain compliance.

Misunderstanding Where Data Is Stored and Processed

Many organizations misunderstand the amount of personal data they store and collect. They assume that all of their customers' PII data is stored in one or two databases, but this assumption is typically incorrect. In fact, companies often unknowingly store data in a myriad of locations. As a result, these companies draw conclusions and establish policies based on inaccurate assumptions around what they think their data storage should be rather than how it actually is processed and stored.

Companies often unknowingly store PII in many locations, including:

Cloud Storage Providers

Databases + Servers

Email

Workstations

COVID-19 Challenges

Due to COVID-19, throughout 2020 many more employees have been working from home. The sudden shift to remote work has left businesses vulnerable to increased risk of data breaches and loss, making it harder to stay compliant with GDPR.

Some circumstances that can put businesses at risk of breaking their compliance include when employees:[8]

- Process, store, or send information through inadequately secured personal devices (e.g. personal mobile phones) or on unsecured Wi-Fi networks
- Transfer documents and data carriers from the office to their homes
- Use tools that do not provide adequate data protection (e.g. unsecured messaging apps)

SECTION 5

Data Discovery: The First Step in Achieving Compliance

Organizations should never take on a “wait-and-see” approach when it comes to compliance: they need to be proactive. The first step in achieving proactive compliance is to develop a baseline understanding of what data your organization has and where it resides: this is a process known as data discovery.

With Enterprise Recon by Ground Labs, GDPR compliance is easily achievable. The award-winning data discovery solution can:

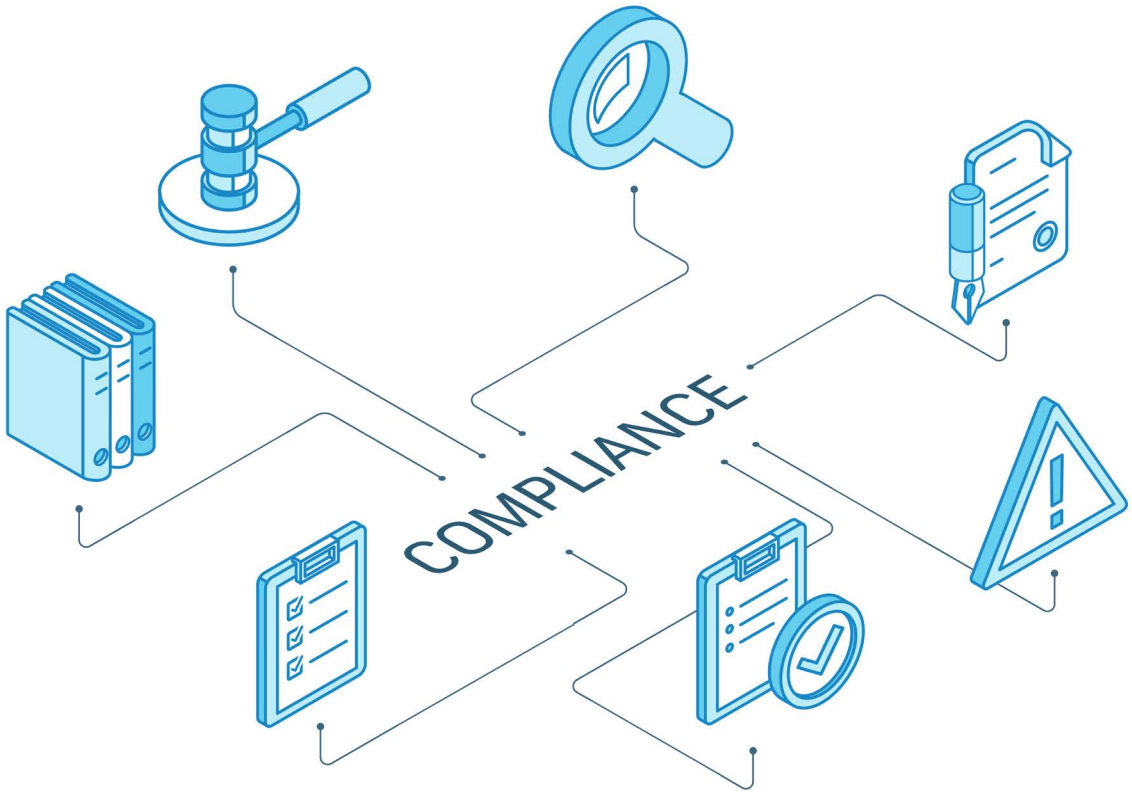
- Identify more than 300 data types of structured and unstructured data including pre-configured, GDPR specific personally identifiable information (PII) patterns
- Demonstrate GDPR compliance with custom reporting and analytics available in the Enterprise Recon
- Scan immediately and quickly thanks to a low-impact distributed design, complementing and strengthening your data loss prevention strategy
- Accurately map data across networks, servers, and platforms to keep tabs on GDPR and PII data and more easily respond to consumer requests
- Easily build custom data types and search platforms to locate and remediate unique data types to address your organization’s unique needs
- Search within both structured and unstructured data sources including files, databases, emails, cloud, big data and more
- Easily view and analyze the access permissions for sensitive data locations and immediately take action to minimize risk by managing and controlling access to those locations
- Establish a ‘Risk Profile’ based on a Risk Mapping/Scoring feature, enabling the tagging of high, medium and low data risks across your network
- Execute a proactive approach to data security — as opposed to a reactive approach that relies on damage control post-breach — to build a stronger foundation of trust within your organization

SECTION 6

Establishing Ongoing Widespread Compliance

Compliance rules are constantly changing, which means that compliance is not a one-time checkmark, but an ongoing obligation. GDPR inspired many other regional privacy laws, like the Australian GDPR and CCPA. In fact, Gartner predicts that by 2023, 65% of the world population's personal data will be protected by various privacy regulations like GDPR.[9]

With Enterprise Recon, organizations can keep up with these ongoing compliance requirements. Enterprise Recon helps companies create an inventory of sensitive data, upholding the GDPR requirement for ongoing data surveillance by monitoring it around the clock via the Enterprise Recon dashboard.



SECTION 7

Conclusion

Ongoing compliance with GDPR is critical for organizations today because failing to comply with GDPR can lead to hefty fines and significant customer loss. The differences between GDPR in the EU and Australia highlight the changing nature of privacy laws, and the importance of keeping up with all relevant regulations around the globe. Adapting to regulations in real-time won't cut it; your team needs to build a system that can handle these changes as they happen. The first step to preparing for ongoing compliance is data discovery.

Are you ready to get your organization better prepared to achieve GDPR compliance? Book a demo with a member of the Ground Labs team by visiting: **https://calendly.com/ground-labs-global-sales-team**

The References

[1] Ben Wolford, “Does the GDPR apply to companies outside of the EU?,” GDPR.EU, https://gdpr.eu/companies-outside-of-europe/.

[2] Ewelina Witek, “GDPR: How to make your business more resilient against data protection breaches in light of the COVID-19 crisis?”, Deloitte, March 2020, https://www2.deloitte.com/ce/en/pages/about-deloitte/articles/how-to-make-your-business-more-resilient-against-data-protection-breaches-during-COVID-19.html

[3] Andrew Dunlop, “GDPR: Personal Data and Sensitive Personal Data,” Burges Salmon, https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data/

[4] “Nader Henein, Bart Willemsen, and Bernard Woo, “The State of Privacy and Personal Data Protection, 2020- 2022,” Gartner, August 26, 2020.

[5] “Ben Wolford, “What are the GDPR Fines?”, GDPR.EU, https://gdpr.eu/fines/.

[6] Scott Ikeda, “First Cross-Border GDPR Fine Comes In; Twitter Will Pay €450,000,” CPO Magazine, December 23, 2020, https://www.cpomagazine.com/data-protection/first-cross-border-gdpr-fine-comes-in-twitter-will-pay-e450000/.

[7] “Cost of a Data Breach Report,” IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

[8] Ewelina Witek, “GDPR: How to make your business more resilient against data protection breaches in light of the COVID-19 crisis?” Deloitte, March 2020, https://www2.deloitte.com/ce/en/pages/about-deloitte/articles/how-to-make-your-business-more-resilient-against-data-protection-breaches-during-COVID-19.html

[9] “Gartner Says By 2023, 65% of the World’s Population Will Have Its Personal Data Covered Under Modern Privacy Regulations,” Gartner, September 14, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w