GDPR Compliance: Is Your Data Center Ready?

On May 25, 2018 the European Union's General Data Protection Regulations (GDPR) will come into effect. The GDPR gives residents of the EU more control over the personal data that is collected online by retailers, healthcare organizations, financial institutions, and who knows who else. The GDPR is the result of a concerted effort to create a comprehensive collection of clear yet flexible regulations that give individuals visibility into their personal data footprints, as well as the power to have personal data erased upon request.

The sanctions for non-compliance are stiff, ranging from a cap of €10 million or 2% of worldwide annual turnover (whichever is greater) for preparedness and administrative failures, to double that for actual breaches or significant compliance failures. Each EU member state can add its own penalties for GDPR-related breaches if there's a gap between the GDPR regulations and their own laws. And individuals can bring civil suits through local jurisdictions if they feel their rights as defined in the GDPR have been breached. In addition to all these financial penalties, an organization that is suspected of noncompliance can be temporarily banned from processing or using data by the GDPR-enforcing Data Protection Authorities.

The GDPR regulations and sanctions apply to all data controllers and data processors (third parties that handle data on behalf of the data controllers, such as public cloud providers) who collect and store personal data related to EU residents — regardless of where the data controller or processor is physically located. This individual-centric approach means that any organization gathering personal data on Europeans, no matter where its corporate headquarters are located, must be GDPR-compliant.

The GDPR is comprehensive — with 11 chapters, 99 articles and 173 recitals. This e-book explores two fundamental GDPR themes and how Our solution's Data Center & Cloud Ops Security Platform can help enterprises address them:

1. **Data Protection**: the requirement for data protection by design and by default (as per Article 25 and Recital 78), and

2. **Data Breach** and the notification obligations in the event of a breach (as per Article 33 and Rectial 85).

Data Protection By Design and By Default

Privacy by Design (PbD) is Not New

The notion that safeguarding the privacy of personal data must be built into software systems from their initial design stage is not new to the GDPR. The European data privacy regulations that the GDPR will be replacing were based on well-established PbD principles such as proactive and preventative data protection (vs. reactive and remedial), privacy embedded into design, privacy as the default setting, protection throughout the data lifecycle, data minimization (i.e., collecting the minimal data required for the purpose), and user-centricity.

However, the PbD-based regulations did not have sanctions. The spread of e-commerce and social media has made it commonplace to gratuitously collect data points that can then be used — by the original data collector or by unauthorized third parties — to create a personal profile that can be damaging in, for example, employment or insurance situations. The time had come for personal data protection regulations that were both clear and enforceable.

GDPR Takes Data Protection to the Next Level

The GDPR defines personal data as any information about a living individual who could be identified from that data, either on its own or when combined with other information. Article 25 and Recital 78 of the GDPR require data controllers to use state-of-the-art technologies and policies to ensure that data protection principles are upheld when designing and implementing applications that collect and process personal data. In addition, the data controller has a clear obligation to let data subjects know how and why their personal data is being processed.

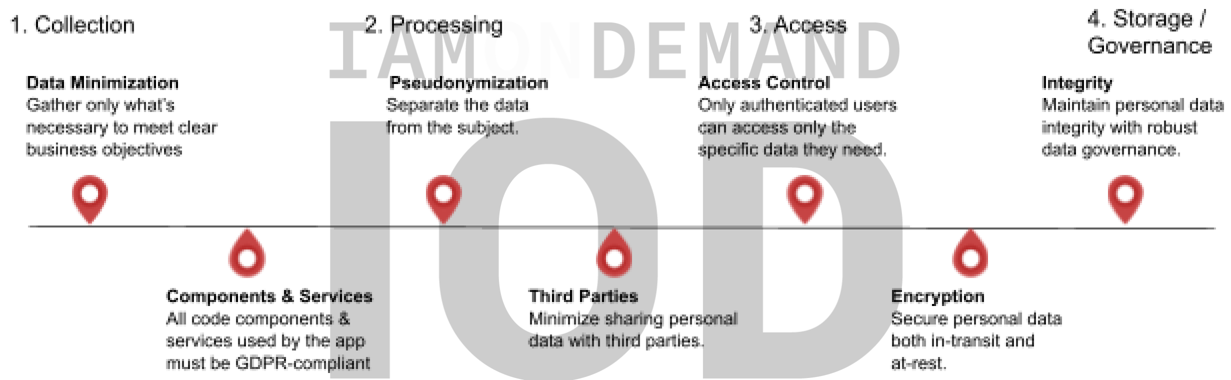
One of the strong points of GDPR is that it does not take a one-size-fits-all approach, but rather adapts its requirements to the type of data being collected. The most sensitive personal data — which require the highest levels of protective measures — can include information on race, ethnicity, biometrics, health, and criminal convictions.

Thus, for example, collecting more sensitive data requires **explicit** permission from the data subject (such as ticking a box “I consent”), while less sensitive data requires only **unambiguous** consent (such as filling in an optional email address). In addition, collectors of sensitive data must offer users the ability to withdraw consent at any time.

Data Protection for Development, Security and Ops Teams

Just as devops teams take security, integration and delivery issues into account from the earliest stages of app design and development, data protection by design means building privacy into the app across the entire data lifecycle (from collection, to usage, disclosure, retention and destruction). In addition, there should be no need for the data subject to take action to achieve data protection, i.e., the highest level of data privacy is the default option.

To meet these requirements, the data controller's development and security teams must carefully evaluate the potential risk to personal data when designing an application's data processing workflow and take measures to mitigate that risk, as illustrated below:



1. Collection

Data Minimization
Gather only what's necessary to meet clear business objectives

Components & Services
All code components & services used by the app must be GDPR-compliant

2. Processing

Pseudonymization
Separate the data from the subject.

Third Parties
Minimize sharing personal data with third parties.

3. Access

Access Control
Only authenticated users can access only the specific data they need.

Encryption
Secure personal data both in-transit and at-rest.

4. Storage / Governance

Integrity
Maintain personal data integrity with robust data governance.

It is also important to constantly monitor and test data security technologies and policies, including maintaining detailed incident reports and other audit trails should it become necessary to demonstrate compliance.

Last but not least, GDPR's demand for high levels of transparency and visibility for the data subject is going to be a major challenge for operation teams. In a recent survey conducted across 1,000+ companies in leading European markets, 12% of the respondents were not confident they know where all their data is stored, while 15% were not confident they have accounted for all databases that contain personal data. Large enterprises expect to get ~250 GDPR inquiries per month, for which they will need to search 43 databases. Assuming seven minutes per search, that translates into nearly 60 hours of searches per working day. Without super-robust data visibility tools, ops teams will be unable to keep up with the demand.

Your GDPR Obligations if Data is Breached

How GDPR Defines a Reportable Data Breach

The GDPR defines a personal data breach as “a 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.”

Article 33 and Recital 85 stipulate clearly that the data controller must notify the competent supervisory authority **no later than 72 hours** after becoming aware of a breach of personal data. Similarly, a data processor must notify the data controller “without undue delay” after becoming aware of a personal data breach.

The main concern is that a personal data breach that is not dealt with in a timely and appropriate manner could result in extensive damage to the data subjects affected. Some of the possible economic or social consequences outlined by the GDPR include loss of control over their personal data, identity theft or fraud, discrimination, or damage to their reputation. A personal data breach may even expose the data subject to legal repercussions by releasing data that they had undertaken to keep confidential.

However, the GDPR rewards data controllers who can demonstrate that they have properly implemented “data protection by design and default” by exempting them from reporting data breaches. The rationale is that the data protection measures put into place ensure that even if data is breached, it does **not** endanger the rights and freedoms of the data subjects affected.

Recital 85, “Notification obligation of breaches to the supervisory authority”, makes it very clear why it is so important that a personal data breach be dealt with in a timely manner:

> *A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*

Reporting a Data Breach

The GDPR is very clear that the obligation of reporting to the supervisory authority within 72 hours falls squarely on the shoulders of the data controller. The supervisory authorities are independent public authorities nominated by the EU member states to be responsible for overseeing the application of the GDPR in their jurisdiction. Although it could be interpreted that the competent supervisory authority is where the breach took place, at the moment the working assumption is that the competent supervisory authority is where the data controller has its main place of business.

NOTE: The GDPR requires that “companies that do not have an office in the EU yet provide their products or services within the European Union must appoint a representative in the Union if they process personal data”. The appointed representative handles matters related to data subjects and supervisory authorities.

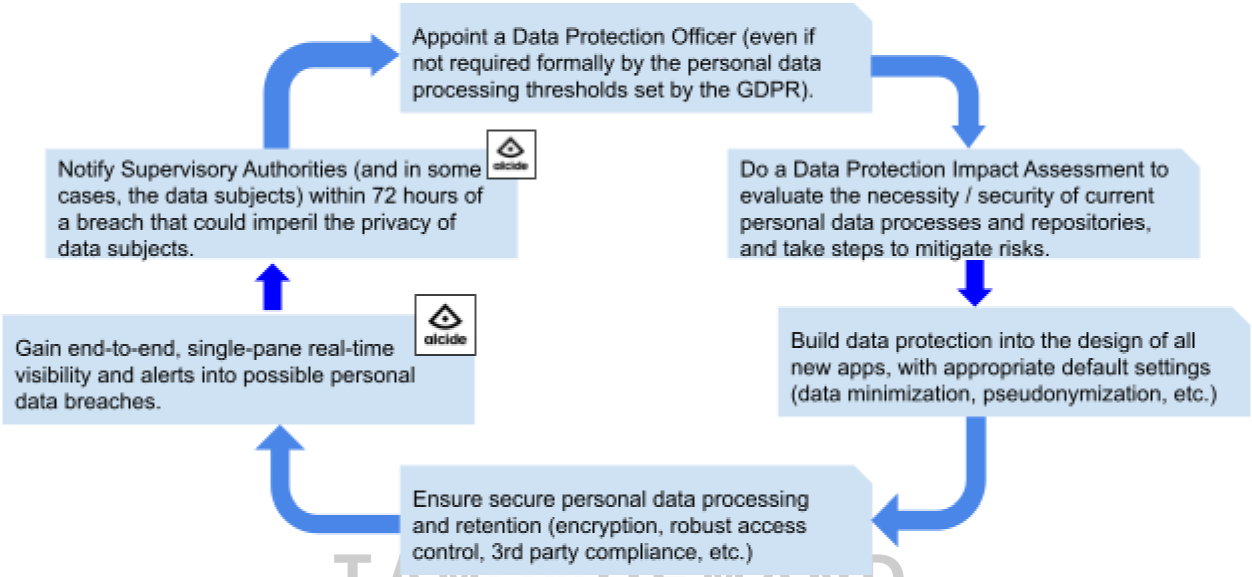
In terms of what has to be reported, the breach notification should describe the nature of the personal data breach as well as approximately how many data subjects it might affect and how. The data controller should also outline measures that have or will be taken to address the breach and mitigate its possible adverse effects.

The GDPR also requires that the data controller report the data breach **to each individual data subject affected by it**. However, there are several substantial exceptions that would free the data controller from this onerous obligation:

- The data has been rendered unintelligible to an unauthorized person who tries to access it — typically through encryption.
- The controller has taken actions to mitigate the risk of the data breach to the rights and freedoms of the affected data subjects, such as pseudonymization.
- When notification to each data subject would involve “disproportionate effort”, in which case alternative communication measures can be used.

In Summary, Be Prepared…

The following decision tree summarizes the steps that an organization should take in order to uphold the GDPR data protection provisions.



Appoint a Data Protection Officer (even if not required formally by the personal data processing thresholds set by the GDPR).

Do a Data Protection Impact Assessment to evaluate the necessity / security of current personal data processes and repositories, and take steps to mitigate risks.

Build data protection into the design of all new apps, with appropriate default settings (data minimization, pseudonymization, etc.)

Ensure secure personal data processing and retention (encryption, robust access control, 3rd party compliance, etc.)

Gain end-to-end, single-pane real-time visibility and alerts into possible personal data breaches.

Notify Supervisory Authorities (and in some cases, the data subjects) within 72 hours of a breach that could imperil the privacy of data subjects.

A Final Note

The sanctions for GDPR non-compliance are very high. Today's complex, hybrid infrastructures consist of endless combinations of data centers and multi-cloud providers, which make it particularly challenging for enterprises to achieve compliance. It is no wonder, then, that the GDPR expects data controllers and data processors to put into place state-of-the-art solutions to ensure the protection of private data — solutions that can show where sensitive data is stored in real-time, map the access points to this data and alert immediately when an anomaly or detection of malicious activity occurs.

Our solution's Data Center and Cloud Ops Security platform provides all stakeholders — development, operations and security teams — with the visibility and detection capabilities they need to enforce policies that will uphold data protection by design, as well as understand and respond to the security threats that endanger the integrity of collected personal data.

Specifically, our platform supports GDPR compliance through:

- Our solution Policy Control and Enforce, which helps security and devops design and build the right security blocks to mitigate privacy risks.
- Our solution access segmentation and segregation policies, which help meet compliance requirements and assure that only approved access is allowed to servers holding personal data.
- Our solution advanced threat protection capabilities, which minimize the time to identify anomalies and potential breaches.

Contact our data security experts to learn how Our solution can help your enterprise effectively meet GDPR requirements — and thus avoid the costly consequences of non-compliance.