SailPoint

SOLUTION BRIEF

# Step-by-Step Guide: GDPR Compliance with Identity Governance

The new EU General Data Protection Regulation (GDPR) represents the most significant change in global privacy law in 20 years. It introduces new and wide-ranging privacy requirements for any organization handling the personal data of individuals living in the EU. The GDPR will broaden and add requirements to its predecessor, the EU Data Protection Directive or DPD, and because it is a regulation, not a directive, it will have binding legal force throughout every member state.

The GDPR was adopted in April 2016 and goes into effect on May 25, 2018. Given the complexity and detailed requirements of the regulation, organizations need to begin now to plan, budget, and implement the process and technology changes needed to meet regulatory guidelines.

**Some key changes that will be enacted by the GDPR include:**

1. Worldwide application of a European data protection law. The new law is not limited to EU member states. No matter where they are located, organizations located outside the EU that process the personal data of individuals residing within the EU will have to comply with GDPR.
2. Tougher sanctions for non-compliance. Under the new legislation, organizations can incur fines of up to €20 million or 4% of annual gross revenue, whichever is greater, depending on the nature of the violation.
3. A new data breach notification requirement. Organizations will now have to notify the relevant European data protection authority of a breach within 72 hours. A notification must also be made to the individuals affected without undue delay when there is a high risk to them.
4. New data privacy governance, data mapping and impact assessment requirements. Many organizations will now need to appoint a data protection officer (DPO) to be responsible for implementing and monitoring compliance with the GDPR and performing compliance assessments. Organizations will also be required to map their processing of EU personal data and undertake data protection impact assessments for higher-risk processing.
5. A requirement to implement "privacy by design." Organizations must take a proactive approach to ensure that appropriate standards of data protection are built into all systems and processes that handle personal data.

An important note is that identity and data access governance meet several requirements of this regulation, and can help prepare your organization for GDPR compliance.

## What Does the GDPR Mean for Security Professionals?

As those who have studied the details of the GDPR know, the regulation is a legal framework that does not specify many technical details as far as how to achieve compliance. However, it does clearly spell out a new set of data protection principles and procedures that must be followed.

In order to get started with GDPR requirements, organizations need to have a clear understanding of how they process, store and secure personal data. Once the organization has catalogued all personal data used for processing, it must ensure that this data is adequately secured. The GDPR mandates that "appropriate technical and organizational measures" be put in place to protect data, and it requires documentation that demonstrates this compliance. Lastly, the GDPR requires organizations to monitor and detect any breaches of personal data that occur and to notify authorities and in some cases data subjects when a breach occurs.

## How Identity Governance Can Help

The right identity governance strategy can help organizations meet GDPR requirements in a sustainable and cost-effective manner. Identity governance provides centralized visibility and control over "who has access to what." It provides a mapping of which users, in what roles, can access applications and data (both structured and unstructured data). As such, it is one of the most valuable tools an organization can have to catalog systems, applications, databases, both on-premises and in cloud, and to determine whether appropriate access controls and safeguards are in place for these resources.

The key elements of identity governance – data access governance, compliance controls, automated provisioning and password management – play key roles in identifying personal data, securing that data and showing proof of GDPR compliance – across the entire organization.

- **Data Access Governance:** automates the discovery and classification of personal data and provides activity monitoring to improve risk mitigation and understand appropriate use.
- **Compliance Controls:** allows organizations to define and enforce access policies, to conduct regular access reviews by data owners and to automatically revoke inappropriate access. Provides centralized reporting of all preventive and detective controls.
- **Automated Provisioning:** ensures that access to personal data is granted on a need-to-know basis only and provides approval workflow and policy checking for any proposed access changes.
- **Password Management:** enforces strong password policies across all systems containing personal data.

**The specific areas where identity governance can help organizations prepare for and meet GDPR requirements are shown below:**

Step 1

## Personal Data Protection Principles

The primary objective of the GDPR is privacy: the protection of personal data. That means the spotlight is now focused on how organizations process, store, and secure personal data. In order to meet GDPR requirements, organizations must demonstrate compliance with the data protection principles defined in Article 5.

### GDPR Article 5 – Data Protection Principles

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

### How Identity Governance Can Help

**Provides Visibility to Personal Data**

- What personal data is being stored?
- Where and how is it stored?
- Who is responsible for it?
- Who can access to it?
- Who has accessed it?
- When does this data expire?

**Controls and Protects Personal Data**

- Removes personal data stored in inappropriate or redundant locations.
- Removes personal data that has not been accessed in a specified time period.
- Removes personal data that has expired.
- Assigns data owners and perform regular access reviews.
- Keeps access rights to personal data to a minimum.
- Detects and revokes inappropriate access rights.
- Detects and revokes stale and unused access rights.

Step 2

## Securing Personal Data

The GDPR requires organizations to implement appropriate technical and organizational measures for securing personal data. In particular, organizations must "design in" measures to ensure data protection compliance. This means that for each new or existing product or service, organizations must ensure that the relevant product or service is designed with data protection compliance in mind.

### GDPR Articles 25 and 32

**Data Protection by Design and by Default**

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

**Data Security**

The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate:

- The pseudonymization and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

### How Identity Governance Can Help

**Strengthens Controls**

- Provides centralized visibility into the access control models for all resources storing and processing personal data.
- Assigns data owners to all resources containing personal data.
- Enables fully automated review of access rights across all resources containing personal data.
- Automatically scans resources to discover and report on any access policy violations.
- Enforces strong password policies across all systems containing personal data.

**Ensures Ongoing Compliance**

- Uses role-based access control to ensure access to personal data is granted on a need-to-know basis ("least privilege").
- Automatically detects job changes such as transfers or terminations and launches the appropriate workflow to remove or change access privileges.
- Requires manager or data owner approval for all access changes.
- Prevents policy violations by evaluating any proposed access changes against defined rules.
- Logs all access requests and actions by approvers, providing a complete and auditable record of who requested access to which systems and who approved or denied the request.
- Provides extensive reporting capabilities to enable self-assessment and provide proof of GDPR compliance.

Step 3

## Monitoring and Detection

The GDPR requires organizations to implement measures to report data breaches to Data Processing Authorities (DPAs) and in some cases to data subjects. The regulation gives companies 72 hours from the time they become aware of a breach to report it, so organizations will need to be prepared to immediately disclose specific details about individuals impacted, the duration of the breach and any remedial actions taken.

### GDPR Articles 33 and 34

**Reporting Data Breaches to DPAs**

- **Controllers** – In the event of a data breach, the controller must report the breach to the DPA without undue delay, and in any event within 72 hours of becoming aware of it. There is an exception where the data breach is unlikely to result in any harm to data subjects. The controller must keep records of all data breaches, comprising the facts and effects of the breach and any remedial action taken.
- **Processors** – Processors must notify any data breach to the controller without undue delay.

**Reporting Data Breaches to Data Subjects**

In the event of a data breach causing high risk to data subjects, the controller must notify the affected data subjects without undue delay. However, the controller may be exempt from this requirement if:

- The risk of harm is remote because the affected data are protected (e.g., through strong encryption);
- The controller has taken measures to protect against the harm (e.g., suspending affected accounts); or
- The notification requires disproportionate effort (in which case the controller must issue a public notice of the breach).

### How Identity Governance Can Help

**Automates Detection**

- Monitors who is accessing personal data, when, from where, and what types of operations they are performing.
- Allows customized definition of access policies and monitors for policy violations.
- Notifies and alerts data owners and managers to any detected violations or anomalies.
- Automates remediations when violations are detected.
- Enables data owners to perform real-time risk status checks over data they manage.

**Provides Complete Audit and Forensics**

- Provides fine-grained audit trails required to conduct forensics in the case of a data breach.
- Logs all changes to access, providing a complete and auditable record of who requested access to which systems and who approved or denied the request.
- Provides audit reports with detailed views of all data access activity, permission changes, and potential non-compliant activity.

Step 4

## Meeting Compliance Documentation Requirements

The GDPR requires organizations to maintain an Internal Data Processing Register to document all personal data processing activities. These rules require both controllers and processors to create a centralized registry that documents data processing activities and describes the technical and organizational security measures taken to protect personal data.

Organizations must also have in place a process for determining when a Privacy Impact Assessment (PIA) is required for "high-risk" processing of personal data. This requirement adds the need to demonstrate that appropriate measures have been implemented with regard to the identification of the risks related to the processing; the assessment of the nature, likelihood, and severity of risk; and the documentation of best practices implemented to mitigate risks.

### GDPR Articles 30 and 35

**Internal data processing register for controllers**

Each controller must keep records of the controller's processing activities, including:

- The categories of data subjects and personal data processed.
- The categories of recipients with whom the data may be shared.
- A description of the security measures implemented in respect of the processed data.

**Privacy Impact Assessment**

Controllers must carry out privacy impact assessments where a type of processing is likely to result in a high risk for the rights and freedoms of individuals. A PIA should include:

- A systematic description of the processing operations and purposes of the processing.
- An assessment of the necessity and proportionality of the processing operations.
- An assessment of the risks to the rights and freedoms of data subjects
- Measures envisaged to address the risks.

If a PIA indicates that processing would result in a high level of risk in the absence of measures taken by the controller to mitigate the risk, the controller must consult the Supervisory Authority prior to the processing.

### How Identity Governance Can Help

**Streamlines Reporting Requirements**

- Identifies personal data stored in hard-to-find locations such as file servers, portals, mailboxes, and cloud folders.
- Provides complete visibility into the access control models for each resource storing or processing personal data.
- Assigns application/data owners to each resource processing personal data.
- Flags processes or data stores with high-risk personal data.

**Assesses and Mitigates Risk**

- Automates the periodic review of access to personal data by managers and data owners.
- Provides detailed reports of each access review cycle including inappropriate access detected, access revocations, and policy violations detected and remediated.
- Uses role-based access control to ensure access to personal data is granted on a need-to-know basis ("least privilege")
- Enforces strong password policies across all systems containing personal data.
- Automatically scans resources to discover and report access policy violations.
- Provides extensive reporting capabilities to enable self-assessment and provide proof of GDPR compliance.

By implementing an identity governance solution in the organization, they can be sure that they are not only compliant with the GDPR, but also better prepared to mitigate the risks of a data breach. With the proper foundation and support that the identity governance solution provides, they can "tick the boxes," so to speak, of many GDPR mandates.

## The Power of Identity™

In today's technology world, the risks are more complex and attacks more frequent than ever. Many organizations find themselves struggling to grant business users seamless access to an ever-increasing number of applications, while concurrently confronting more frequent and sophisticated cyberattacks. The tough balance between convenience – enabling users to work how they want, where they want – and maintaining tight control over user access has never been more difficult or more critical.

Today's IT security teams are struggling to manage the explosion of cloud and mobile applications layered on top of the organization's traditional on-premises applications. They must also manage and enable a distributed, global workforce that blurs the lines between employees, contractors and partners. This is all in addition to facing and conquering new regulations that add complexities to how security must function.

To make matters worse, it is no longer enough to focus on defending the organization's application infrastructure and network perimeter. As recent security attacks demonstrate, it is becoming more common for identities to become the attack vector for cyber criminals. Instead of targeting networks and application infrastructures, hackers are now exploiting identities to gain access to sensitive systems and data.

The power that an identity governance program can provide organizations is more than just security. Once enterprises know that through their efforts, the business is safer, more efficient and better protected. They are free to do what they set out to do in the first place: improve the organization. Whether that means gaining a competitive advantage, chasing new opportunities for growth, or providing a better experience for its customers, the empowerment organizations gain with identity governance is what allows them to be confident, fearless and unstoppable.