WHITE PAPER

Complying with the General Data Protection Regulation (GDPR)

ServiceNow Governance, Risk, and Compliance

servicenow

Table of Contents

What is the GDPR?

The General Data Protection Regulation (GDPR) (Regulation [EU] 2016/679) is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It forces stricter responsibilities on organisations to prove that they have adequate processes in place to manage and protect personal data. The major goals of GDPR are protection of an individual's personal data and the definition of the rules for the free movement of personal data in the EU.

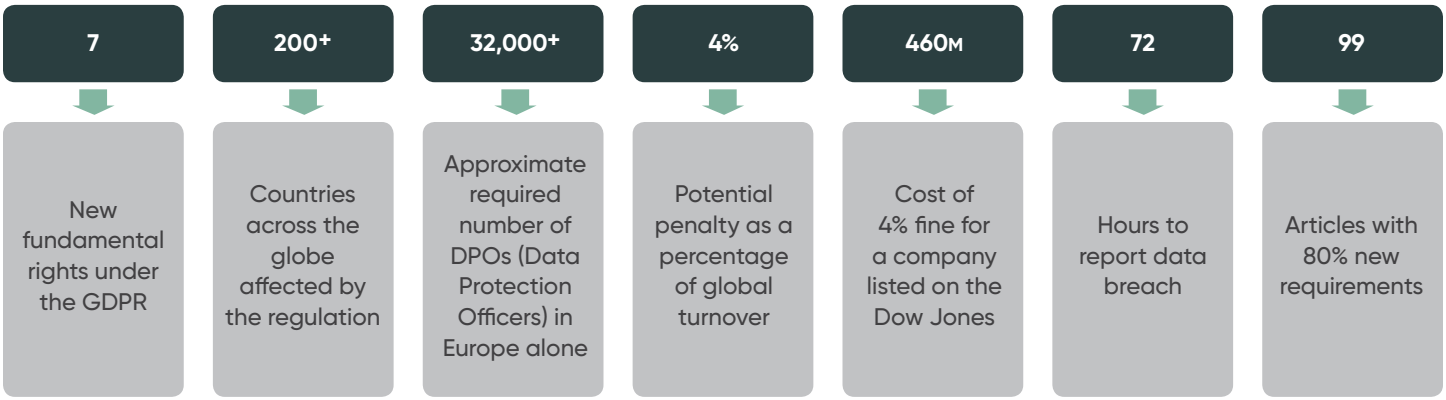
The EU defines "Personal Data" as "any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address." The new obligations pertain to any organisation that handles data about EU citizens—whether that organisation is in the EU or not. The regulation does not apply to the processing of personal data for national security activities or law enforcement ("competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties").

What you should know about the GDPR:

- The GDPR introduces a common data breach notification requirement– within 72 hours
- It's a regulation and not a directive! This means that it does not require any enabling legislation to be passed by national governments
- Appointment of a Data Protection Officer (DPO) is mandatory (in most cases)
- It applies to all organisations operating within the EU
- It introduces mandatory Data Protection or Privacy Impact Assessments (DPIAs)
- There is liability for all organisations that touch any personal data (analogue and digital assets)
- It requires privacy implemented in systems and processes by design
- The GDPR introduces the concept of a one-stop shop (one regulation for all EU members)

Enforcement date: 25 May 2018

> "The major goals of GDPR are protection of an individual's personal data and the definition of the rules for the free movement of personal data in the EU.



Key Requirements for the GDPR

Accountability, Policies, and Procedures

- Mandatory appointment (in most cases) of a DPO responsible for data processing
- Evidence of internal documentation on policies and procedures
- Implementation of special codes of conduct

Compliance and Risk Activities

- Measurement of effectiveness of activities and compliance controls
- Implementation of risk-based approach for data processing
- Definition of all risks presented by a data processing activity
- Likelihood and severity of the risks by data processing activities
- Implementation of DPIAs

Implementation of Security Measures

- Implementation of controls and processes related to potential security threats and breaches
- Pseudonymisation and encryption as suggested controls
- Regular controls to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services
- The ability to restore the availability and access to data and services, in a timely manner, in the event of a security incident
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures; to ensure the security of the processing

> “Under the GDPR, independent Data Protection Officers will be under legal obligation to notify the Supervisory Authority of a data breach as soon as they become aware of it.

Data Breaches

Notification & Reporting Requirements

Under the GDPR, the independent DPO will be under legal obligation to notify the Supervisory Authority (SA) of a data breach as soon as they become aware of the breach (§ 33). The maximum allotted time is 72 hours, in accordance with §55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Individuals must be notified if adverse impact is determined. Information that must be provided is as follows:

- Nature and approximate number of affected records with personal data
- Name and contact details of the DPO or other contact point
- Likely consequences of the personal data breach
- Measures taken or proposed to be taken to address the personal data breach; where appropriate these should include measures to mitigate its possible adverse effects
- Documentation of any personal data breaches including: the facts relating to the personal data breach, its effects, and the remedial action taken. The documentation shall enable the SA to verify compliance with §33

Some additional information that is important to keep in mind when reporting a breach

• The GDPR also relates to the security of personal data and data breaches, and thus to Enterprise Security Response (ESR)

• In case of a breach, speed is critical–both the Mean Time To Identify (MTTI) and the Mean Time To Remediate (MTTR) metrics are important

• It´s crucial to understand the scope of the breach, the affected data, systems, and business processes. This insight helps to understand whether a notification is needed or not

Potential Penalties

• A warning in writing in cases of first and non-intentional non-compliance. It is important to prove that it was unintentional!

• Regular periodic data protection audits (collection of relevant evidence)

• A fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (§83, Paragraph 4)

• A fine up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (§83, Paragraph 5 & 6)

Reporting

• Reporting on compliance state and metrics of implemented policies, procedures, and relevant controls and data protection audit evidences

• Capturing and recording activities during incident handling is important

• Automatic documentation, including post-incident reports that simplify and speed up the process

> “
>
> In case of a breach, speed is critical– both MTTI (mean time to identify) and MTTR (mean time to remediate) metrics are important.

Best Practises to Address the GDPR Requirements

Establish

• Involve the stakeholders of your organisation and get their buy-in to successfully implement the GDPR requirements

• Make a checklist of requirements

• Establish and amend organisational policies and procedures to match the GDPR requirements supporting CIAR (confidentiality, integrity, availability, resiliency)

• Establish a DPO and GDPR project and accountability team

• Educate teams responsible for addressing the GDPR requirements

Connect

- Create policy enforcement procedures for compliance requirements
- Implement technologies to prevent and detect security threats
- Operationalise risk, security, and compliance controls

Scope

- Discover what personal data is collected and how it is used
- Detect and assess changes to risk and security posture, in real time
- Analyse both the severity of the data breach and business criticality
- Scope and calculate potential financial impact in case of a data breach

Operationalise

- Implement regular auto-executions of GDPR controls for related citations
- Leverage risk and security data for audit planning
- Engage regular periodic data collection and protection audits
- Accelerate remediation and orchestration through automation

Measure and Report

- Get real-time, business insight into the enterprise's compliance, security, and risk posture
- Track the status of audit, compliance, and remediation tasks at the business service, risk, security, and impact level
- Quickly review the business services that are the most out of compliance
- Identify areas most under duress and determine if the issue is technical, training, or personnel related

Vision

- Align priorities with business elements that are vital for GDPR compliance
- Enhance security and risk management resources—educate
- Optimise costs and productivity from lessons learned
- Establish resiliency procedures through post-data breach and security incident activities
- Create dedicated knowledge base articles to help responders take care of repeat issues quicker and predict potential future threats/ breaches
- Join the established and relevant Information Sharing Analysis Centers (ISACs) for your organisation

“

Identify areas most under duress and determine if the issue is technical, training, or personnel related.

Basic Questions You Need to Answer

Do you understand how your business uses data?

You need to understand what data you have and how it is being used. This can be achieved by conducting a data use and security audit. Can you adequately address the following questions?

- What types of personal data do you collect and use?
- Do you hold sensitive data such as health information?
- What types of processing do you undertake?
- Do you make any decisions based on automated processing or profiling of individuals?
- Where will data be stored? How secure is it? Who has control over the data? Will personal data be transferred outside the EU?

Do you need to strengthen and design new policies and systems for GDPR compliance?

You need to make sure IT systems, staffing, policies, and contracts are compliant with the new rights and responsibilities. Privacy policies need to be rewritten with additional information in simple terms. Some questions to think about are:

- What would you do if customer or employee data was disclosed or destroyed?
- Do you have a policy in place so that employees know what to do if they receive a request for access to personal data or "to be forgotten"?
- Are you clear about the grounds, on which you collect and use data?
- Do you have sufficiently strong methods of obtaining consent?
- What changes should be made to your data controller and data processor contracts?

Can you prioritise and implement key remedial measures using a risk-based approach?

You need to identify issues that pose the highest risk to the business and act to address these first. Privacy impact assessments identify the likelihood of the identified risks occuring and address mitigation strategies.

- What is the degree of harm to individuals?
- What compliance actions are required?
- Are there any high-risk processes, for example involving large quantities of sensitive personal data, which require prior consultation with the DPO?

Are current training plans for your staff on data protection sufficient?

Organisational culture needs to reflect the new approach in the GDPR and enshrine respect for privacy. Some things to think about are:

- Can staff training on data protection be fully embedded in the organisation?
- Do employees know and understand the organisation's data protection policies?
- If confidence is low around employee training, do you need a dedicated DPO to ensure requirements are met?

"You need to make sure IT systems, staffing, policies and contracts are compliant with the new rights and responsibilities.

Get started

The GDPR is a fact, but complying with it can be challenging:

- Responding in 72 hours to data breaches will require significant planning and practise
- Understanding the applicability of the key requirements of the GDPR to an organisation creates additional work. Activities include creating attestations required for key stakeholders and other involved parties including third party vendors
- Consideration of policies, procedures, and technology to meet the GDPR requirements
- Lack of GDPR experts, knowledge, and resources
- Education in data protection and privacy is a critical success factor for the GDPR
- Creating the communication method context to an SA
- Compiling audit evidences from across business units, departments, stakeholders
- The implementation of the EU GDPR will require comprehensive guidance, domain knowledge, and in many cases, changes to business practises
- Implementation enforcement by the EU and tracking

Alignment of your data handling practises with the GDPR is mandatory. Familiarise yourself with the GDPR challenges and requirements while collecting and using personal data, then map those to your organisational policies and procedures. Understand the impact of the GDPR, educate and train your people; and get professional guidance if necessary. Finally, evaluate technologies that can help you and implement best practises.

> “
> Alignment of your data handling practices with the GDPR is mandatory.

ServiceNow Can Help

ServiceNow Governance, Risk, and Compliance is an ideal solution to address the GDPR. It can identify the applications that touch personal data and provide a means to gather evidence; tracking compliance of those applications across functional groups. Capabilities include:

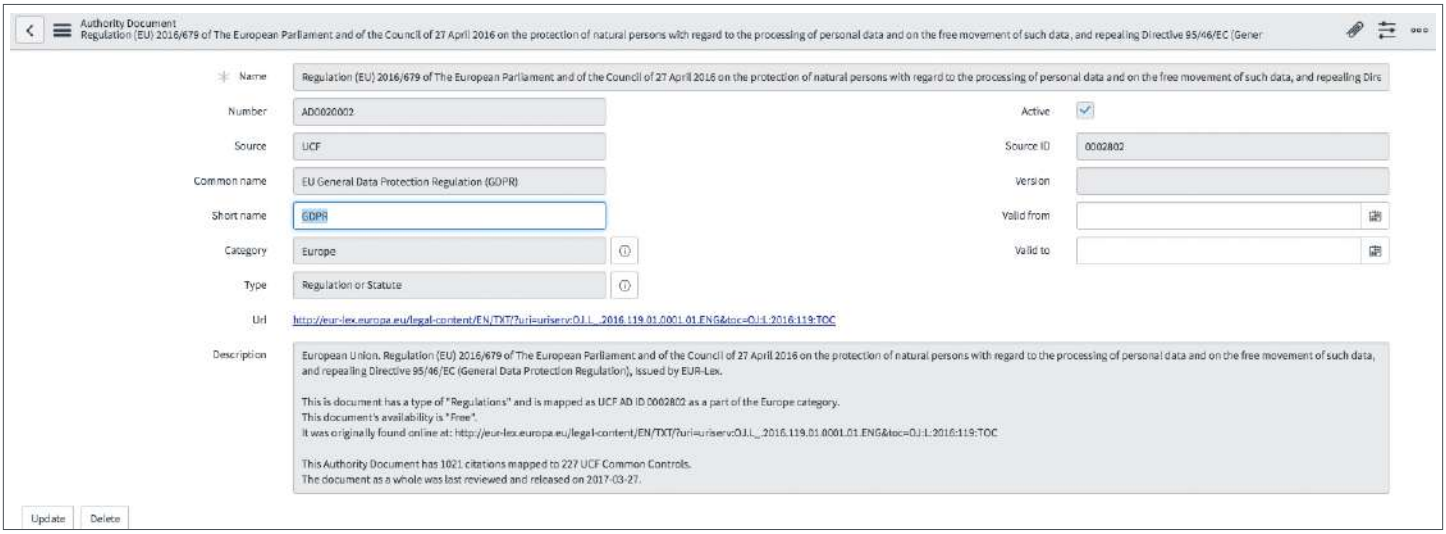
1. Import GDPR requirements and description and Policy Management
2. Data Protection Impact Assessments (DPIAs)
3. Risk evaluation and management requirements
4. Audit requirements
5. Data subject requirements
6. Personally Identifiable Information (PII) mapping
7. 72-hour breach notification
8. Manage third-party GDPR compliance
9. Data Protection Officer (DPO) dashboard

1. Import GDPR requirements and description

The EU GDPR has published a requirements catalogue on their website, it contains 99 articles and 1021 citations. The GDPR Information site provides the regulation scope in 28 languages and can be downloaded from: **EU GDPR Official Web site**

ServiceNow GRC can import all the GDPR requirements with descriptions and guidance with available UCF integration. A license to import the GDPR content from the Common Controls Hub is required. ServiceNow can then map the identified GDPR requirements for an organisation directly into the application, with underlying citation and controls needed for compliance checks and continuous monitoring.

> “ServiceNow offers full policy lifecycle management.



Policy management

Organisational policies need to be aligned with the GDPR requirements. Policy management is associated with the GDPR requirements: (§4.20: Binding Corporate Rules (BCRs); §24.2: Responsibility of the controller; §39.1b: Tasks of the data protection officer). Depending on the GDPR compliance requirements, multiple policies may need to be developed, and existing policies amended or aligned to the GDPR. Some policy examples include: data protection policy, security policy, and code of conduct.

ServiceNow offers full policy lifecycle management. Drafting a policy according to requirements through review, approval, publishing, and retirement stages are available out-of-the-box. A policy can include in the description the GDPR requirements it is designed to align with. Additionally, knowledge base policy information can be automatically created when publishing the relevant policy.

2. Data Protection Impact Assessments

DPIAs are required to assess processing operations that result in a high risk to data subjects. The DPIA is associated with GDPR requirement §35: Data protection impact assessment. The DPIA and prior consultation requirement states: “The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.”

The assessment shall contain at least:

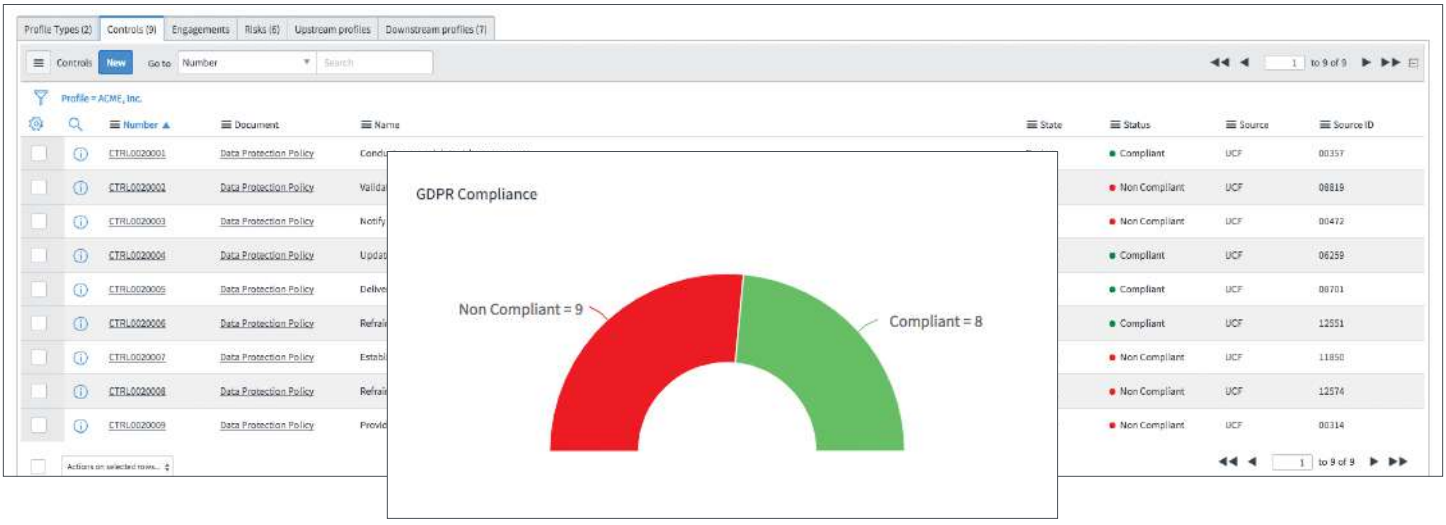
- A systematic description of the envisaged processing operations
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation, taking into account, the rights and legitimate interests of data subjects and other persons concerned

Within ServiceNow GRC, data protection assessments can be aligned with data protection policy and underlying requirements. All assessment requirements can be built with the Assessment Designer or enhanced with existing data protection assessments. The assessments can be scheduled on a regular basis with the outcome reflecting the compliance status of data protection.

The compliance status is reported in real time on the Policy & Compliance Management dashboard allowing for immediate remediation. Meanwhile, the controls status is automatically updated and for any non-compliant outcomes, an issue is automatically created and assigned to the responsible team member to close the requirements gap.

“

Within ServiceNow GRC, data protection assessments can be aligned with data protection policy and underlying requirements.



3. Risk evaluation and management requirements

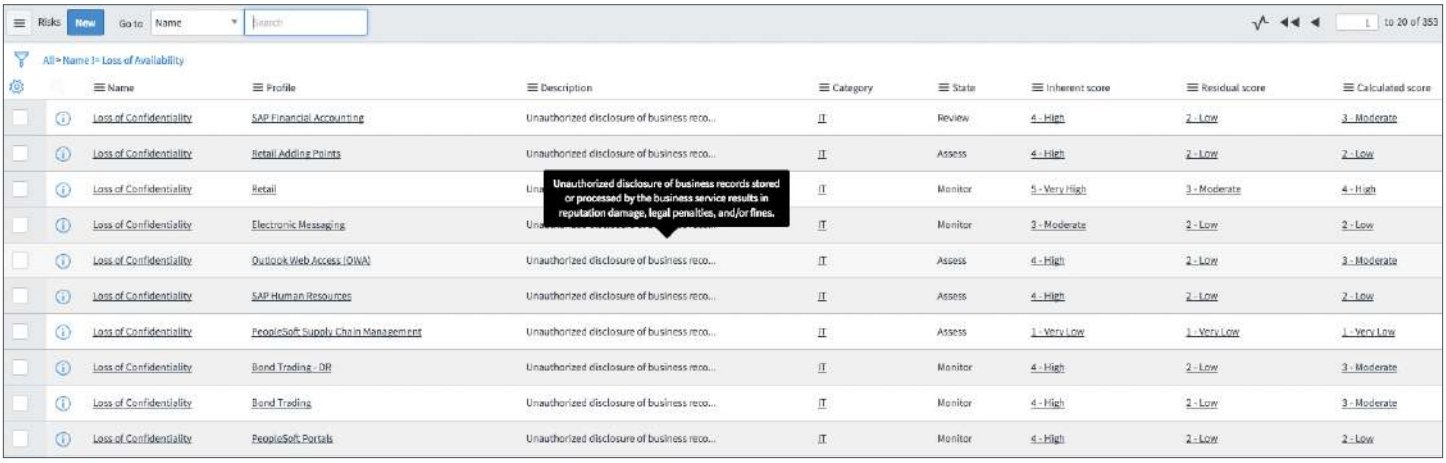
The GDPR requires organisations to appropriately evaluate and manage data protection risk. This is associated with several GDPR requirements:

- Recitals 76, 77,85 contain:
  - Risk should be evaluated on the basis of an objective assessment
  - Guidance on the implementation of appropriate measures and on the demonstration of compliance especially as it relates to the identification of the risk
  - Notification to an SA on a breach with associated risks

- §24: Responsibility of the controller
  - Purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons; the controller shall implement appropriate technical and organisational measures to ensure; and to be able to demonstrate that processing is performed in accordance with this regulation
- §25: Data protection by design and by default
  - Implement appropriate technical and organisational measures, such as pseud-onymisation, which are designed to implement data protection principles, such as data minimisation
- §32/ 33: Security of processing
  - Ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- §33/34/ 35: Notification of a personal data breach to the SA/communication of a personal data breach to the data subject
  - Risk assessments concerning protection measures applied
  - Controller shall communicate the personal data breach to the data subject without undue delay
- §57/ 70: SA and European Data Protection Board (EDPB) tasks
  - Promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing

> “
>
> Promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing.

ServiceNow provides a full risk management lifecycle process, in which regular risk assessments can be implemented and assigned automatically. Risk identification and compliance statistics can be made transparent, and a notification can be sent automatically or manually to an SA at the time of a breach with the associated risks. Data processing on the Information layer with personal data can be implemented. Pseudonymisation and encryption functionalities from ServiceNow help address compliancy requirements with the GDPR. Finally, ServiceNow GRC provides controls to check Confidentiality, Integrity & Availability of systems and applications.



4. Audit requirements

Organisations will need to constantly monitor compliance with the GDPR. This is associated with the GDPR requirements:

- §39: Data protection officer and tasks
  - DPO to monitor compliance with this regulation and related audits
- §47: Binding Corporate Rules (BCRs)
  - Establish data protection audits
  - Mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject
  - Mechanisms for reporting

The ServiceNow Policy and Compliance Management and Audit Workbench dashboards provide the ability to monitor the global level of compliance to the GDPR. Compliance activities can be filtered by entities, systems, and units. ServiceNow GRC can design and schedule regular GDPR audits targeting the organisation and its personal data sensitive systems. In addition, it can generate remediation plans and track data protection corrective actions to conclusion.

5. Data subject requirements

Data subjects have specific rights over the processing of personal data. A variety of requirements are associated with this:

- Chapter 3: Rights of the data subject
  - §13: Information to be provided where personal data are collected from the data subject
  - §14: Information to be provided where personal data has not been obtained from the data subject
  - §15: Right of access by the data subject
  - §16: Right to rectification
  - §17: Right to erasure ("right to be forgotten")
  - §18: Right to restriction of processing
  - §19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
  - §20: Right to data portability

You can utilize ServiceNow Customer Service Management (CSM) module and the Service Portal to interact with data subjects (e.g., customers, staff, third parties, or contacts), providing access through its portal. The portal could include GDPR related information such as policies, procedures, and requests. It could also share data and collect decisions (e.g., opt-in, opt-out, rectification, or process limitations) from data subjects.

> "The ServiceNow Policy and Compliance Management and Audit Workbench dashboards provide the ability to monitor the global level of compliance to the GDPR.

6. Personally Identifiable Information (PII) mapping

Protecting personal data or information requires the ability to attest to controls, assess risks, and perform audit assurance for the information assets and the systems supporting them (e.g., databases, operating systems, servers, or applications). You must be able to:

- Map information assets to other configuration items (CIs) in the Configuration Management Database (CMDB)
- Relate controls to information assets
- Relate risks to information assets
- Run audits against information assets
- Assure proper ownership of information assets

You can leverage ServiceNow CMDB to manage information assets, associate them to other CIs, and create profiles to generate risks and controls against them. A few of the capabilities to fulfill personal data asset requirements are: managing risks, continuous control monitoring, and data protection impact assessments on information assets as well as on business services or on IT CIs.

7. 72-Hour breach notification

One of the more difficult requirements of the GDPR is the 72-hour breach notification. Identifying a breach that puts personal data at risk is the first hurdle, then ensuring the appropriate people are notified and implementing a process to adequately track response is the next. In many organisations this takes longer than the allotted 72-hours. It should be noted that the 72-hour limit is only if the breach puts personal data at risk. The following articles are associated with a breach notification:

- Article 33 and 34
  - The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Supervisory Authority (SA), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the SA is not made within 72 hours, it shall be accompanied by reasons for the delay.
  - There must be alignment between security incidents, breach detection, and data protection risks. The following must be available:
    - Description of the likely consequences of the personal data breach
    - The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
    - Implementation of appropriate technical and organisational protection measures

“
You can leverage ServiceNow CMDB to manage information assets, associate them to other CIs, and create profiles to generate risks and controls against them.

ServiceNow GRC and Security Incident Response work together to help ensure breaches are identified quickly and communicated effectively. With ServiceNow:

- Achieve alignment between GDPR breach and data protection risks
- Breach notification elements and related stakeholders can be automatically notified, for example, the Supervisory Authority can be triggered by a workflow or email
- Parallel tasks and activities can be executed
- 72-hour timer can be instituted
- Regulatory compliance status after GDPR breach can be tracked while providing a timely response

8. Manage third-party GDPR compliance

Organisations are accountable for third-party vendor compliance and therefore must ensure their vendors are protecting a data subject's personal information. Article 4 defines the "Processor" as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Article 28 requires the Processor to adhere to certain guidelines:

1. When a third-party is authorised to processes personal data of a data subject they must provide sufficient guarantees that they have implemented appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. Processing of personal data is governed by a contract or other legal act under Union or Member State law and is binding with regard to the subject-matter, duration, nature, and purpose of processing. In addition to the type of personal data.

Implementing ServiceNow Vendor Risk Management provides the capabilities to ensure a vendor is meeting the requirements and protecting a data subject's personal data. Specifically Vendor Risk can help:

- A formalized tiering process
- Manage the vendor portfolio
- Design a library of assessments, based on questionnaires and evidence collection
- Schedule data privacy assessments to vendors, based on tiers or risks
- Connect questionnaire questions to GRC controls, so that the Vendors' response automatically sets the related control to compliant or non-compliant
- Deliver an external Vendor Portal for vendors to freely respond to the Privacy Assessments pushed to them.
- Manage identified issues or actions to resolution to improve the GDPR compliance of vendors

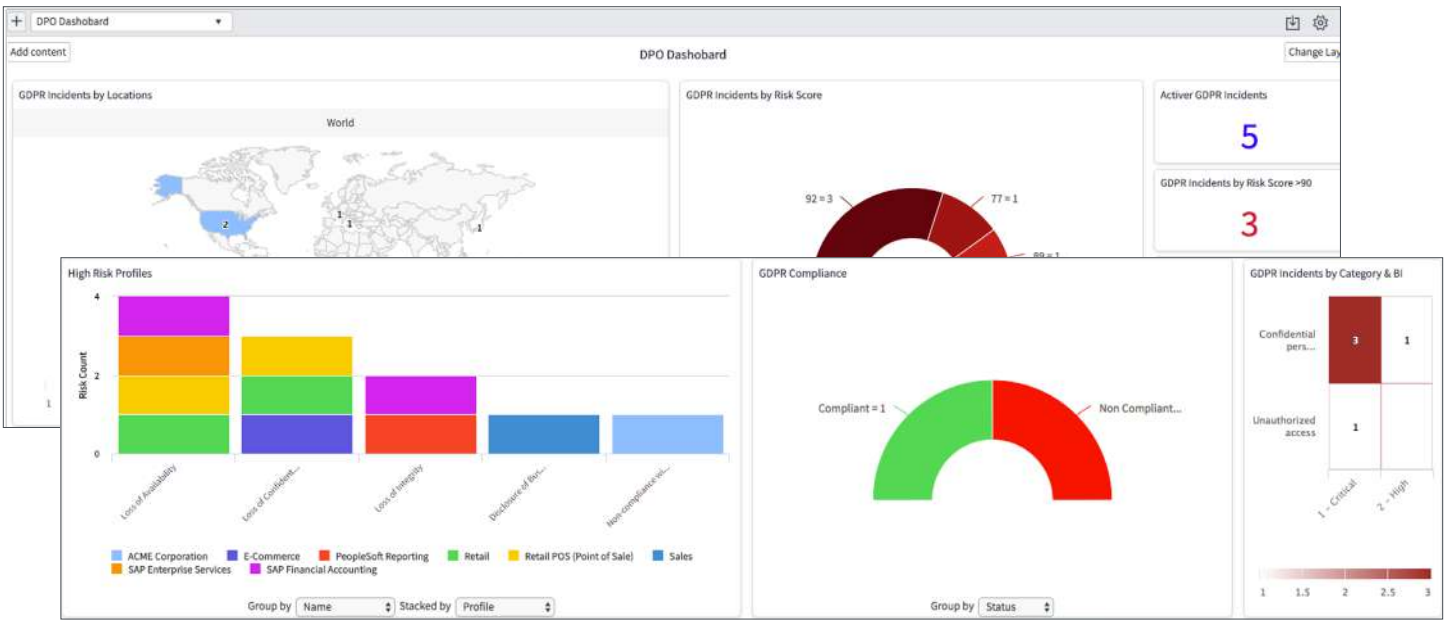
> "ServiceNow Vendor Risk Management helps ensure a third-party is protecting a data subject's personal data.

9. Data Protection Officer (DPO) dashboard

The DPO is the individual in the organization responsible for ensuring compliance and the immediate reporting of breaches. Many larger organizations are establishing this new position. Visibility and transparency, in particular, the ability to accurately track incidents and remediation activities is key for a DPO.

ServiceNow Performance Analytics and the Service Portal offer the ability to create dashboards specific to your role and responsibility in a matter of minutes.

Some examples of possible dashboard metrics are GDPR incidents by location, High Risk Profiles (across vendors, applications, departments, etc.), and Incidents by Business Impact.



What ServiceNow GRC Does Not Do

Please note that ServiceNow Governance, Risk, and Compliance:

- Does NOT do data mining to identify personal data within databases
- Does NOT do data mining to identify personal data within unstructured data
- Does NOT delete or archive personal data for data subjects who would like to be forgotten

For More Information

Speak to your partner or ServiceNow representative for more information or visit our website: **www.servicenow.com/grc**

servicenow

© Copyright 2018 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and /or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.
SN-GDPR-092018