General Data Protection Regulation (GDPR) at SAP

Overview

October 2017

PUBLIC

SAP Run Simple

Legal Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation and SAP's strategy and possible future developments, products and/or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information on this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, and shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document. This limitation shall not apply in cases of intent or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

NOTE: The information contained in this presentation is for general guidance only and provided on the understanding that SAP is not herein engaged in rendering legal advice. As such, it should not be used as a substitute for legal consultation. SAP SE accepts no liability for any actions taken as response hereto.

It is the customer’s responsibility to adopt measures that the customer deems appropriate to achieve GDPR compliance.

GDPR
requirements and impact

What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) (EU Regulation 2016/679), effective 25 May 2018, gives **individuals control** and **protection** of their **personal data**. Data controllers, who determine the purpose and means of processing personal data, and processors, who process for controllers, are affected.

Penalties up to 4% of annual global revenue or **€20 million** whichever is greater

Who must comply?

Organizations that offer goods or services to, or monitor the behavior of, EU data subjects and those that process or hold the personal data of EU residents

Applies to:

Natural persons, whatever their nationality or place of residence in the EU, in relation to the processing of their personal data

GDPR at a glance

Protects fundamental rights related to the processing of personal data

Demonstration of compliance

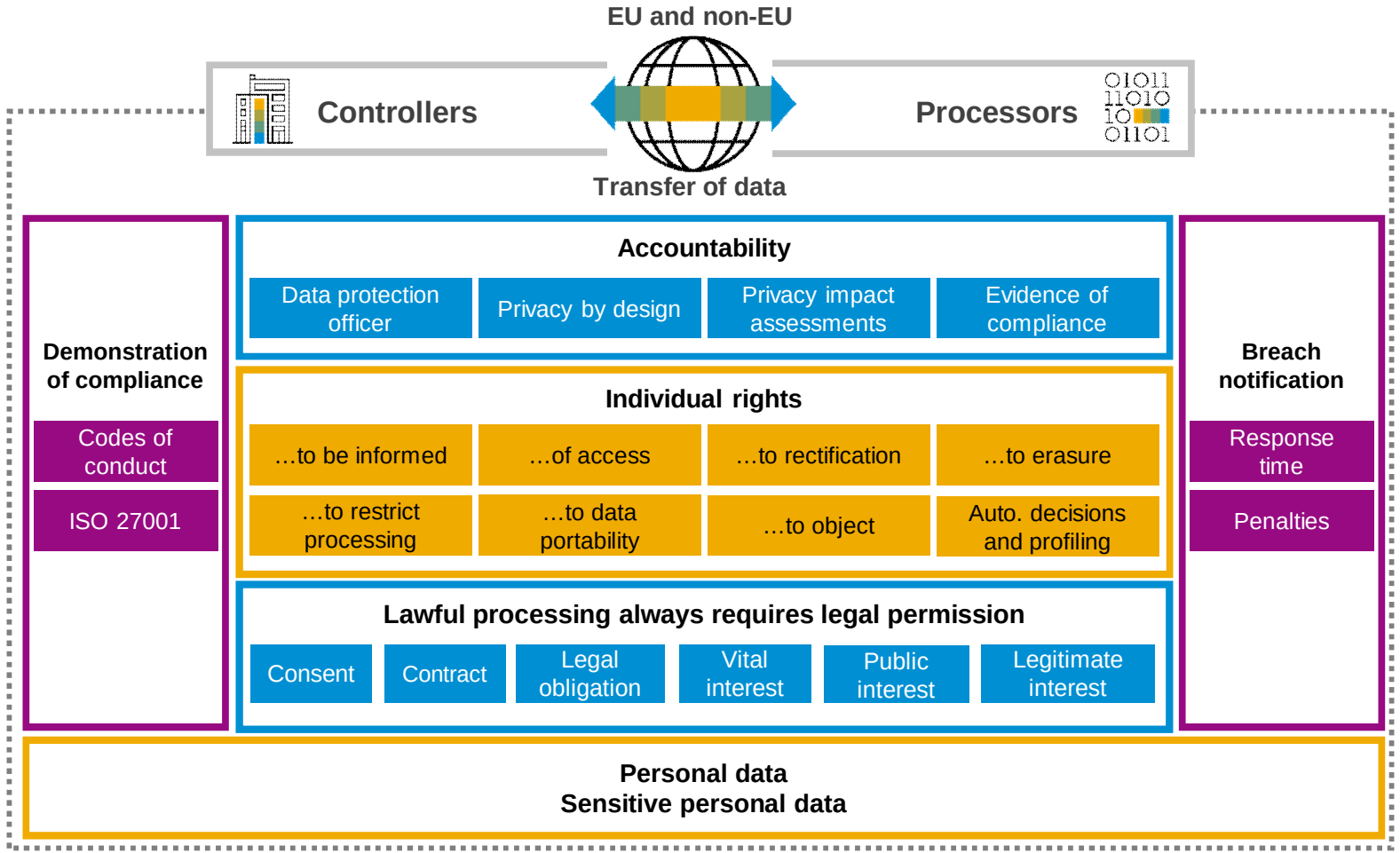
- Compliance and accountability are integral to a data protection program.
- Codes of conduct and policies can help ensure accountability.

Accountability

- Produce and maintain evidence of compliance-supporting actions
- Build data protection into product design and development
- Appoint a data protection officer (DPO) if your company has large-scale processing requirements

Lawful processing

- Requires a legal basis, e.g. a contract, consent, or legitimate interest for the processing of personal data
- Must keep such data accurate and stored only as long as needed



Personal data

- Includes online identifiers, mobile device IDs, IP addresses, and more; may include de-personalized data
- Requires parental consent for children under 16 years

Controllers and processors

- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controller is accountable for failures of the data processor; both controller and processor are liable for breaches.

Breach notification

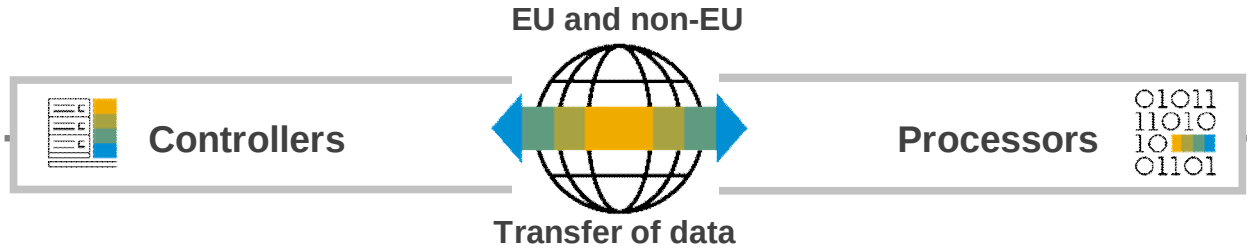
- Mandatory notification to authority within 72 hours of becoming aware of breach
- Communication to affected individuals without undue delay
- Maximum fine can apply

Individual rights

- The GDPR suggests self-service apps for personal data-related information requests
- Rights apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.

GDPR at a glance

Protects fundamental rights related to the processing of personal data

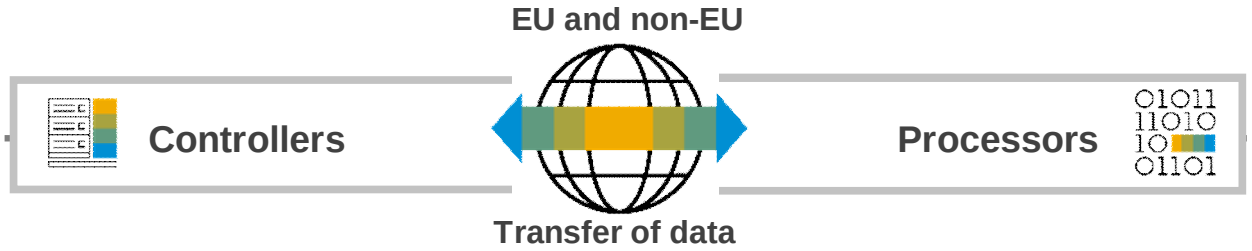


Controllers and processors

- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controllers determine the purpose and means of processing personal data and bear primary responsibility for compliance.
- Processors are those who process personal data on behalf of a controller.
- Controller is accountable for failures of the data processor, and both controller and processor are liable for breaches.

GDPR at a glance

Protects fundamental rights related to the processing of personal data



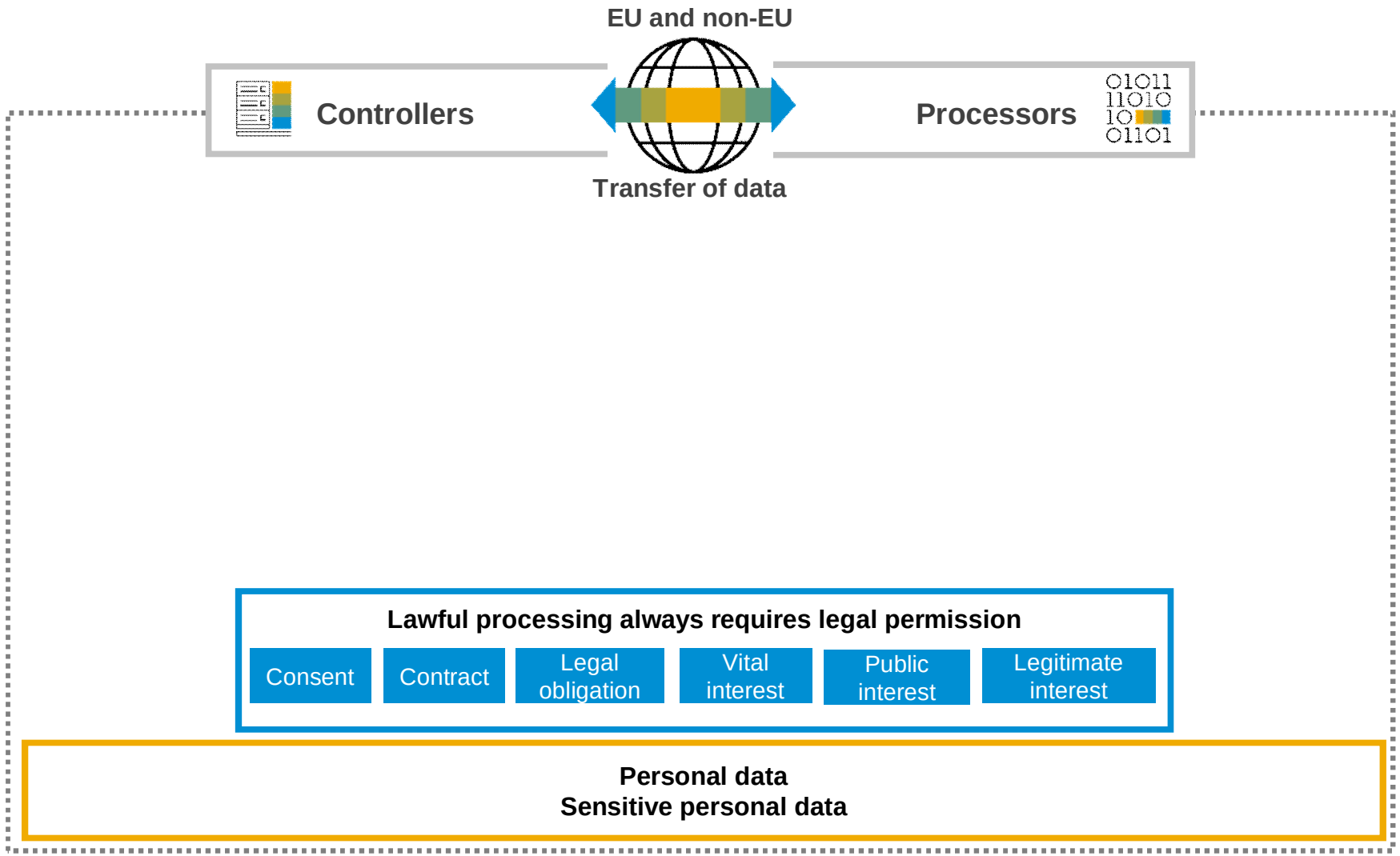
Personal data
Sensitive personal data

Personal Data

- Personal data relates to an identified or identifiable person and includes online identifiers such as name, phone, e-mail address, mobile device IDs, IP address…
- Sensitive personal data includes data such as ethnic origin, biometric or genetic data, or health, and can be subject to more stringent requirements.
- De-personalized data is in scope
- Special categories of personal data may require stronger reasons to process and tougher protections

GDPR at a glance

Protects fundamental rights related to the processing of personal data

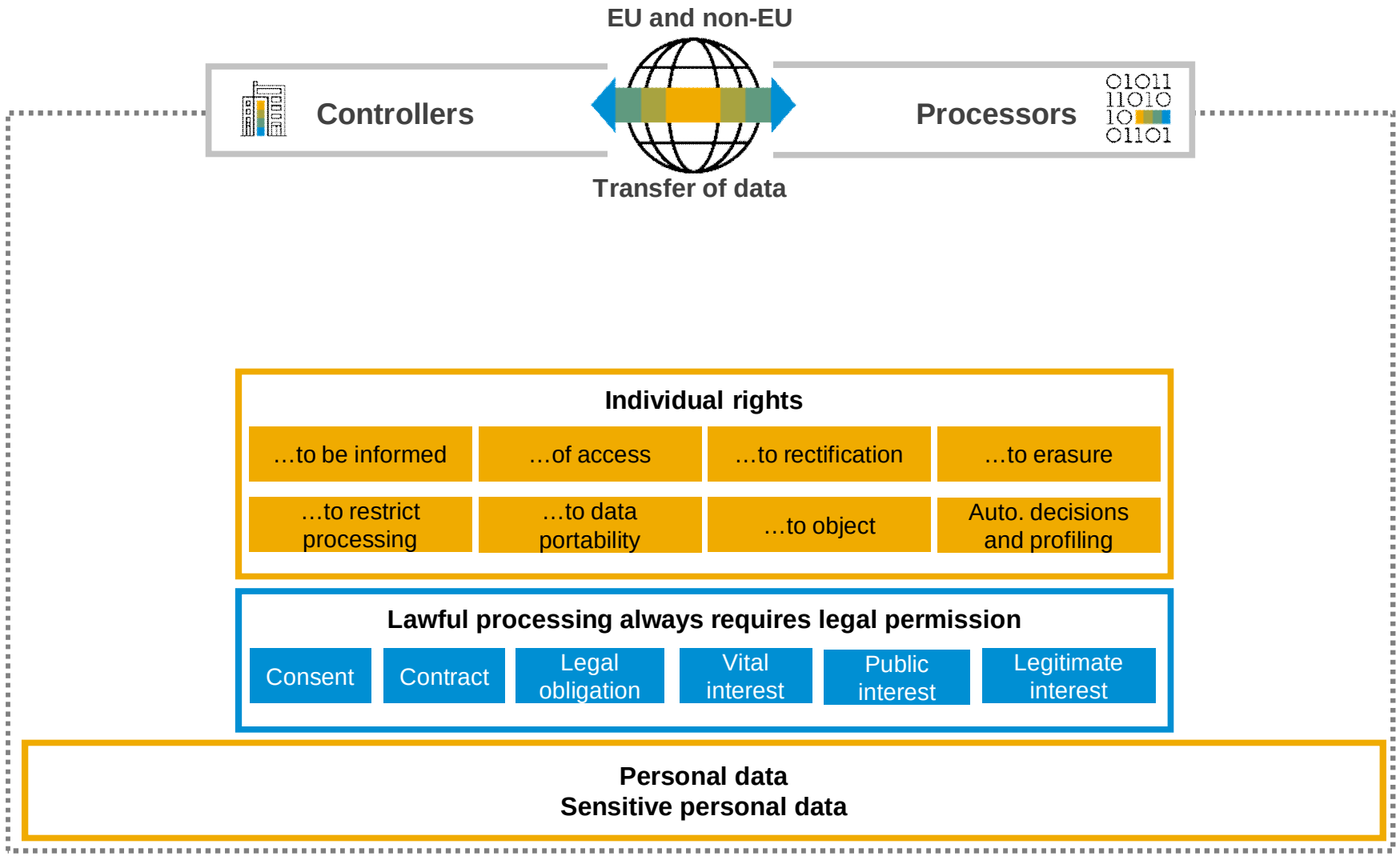


Lawful processing

- In general, there must be a legal basis, like a contract, consent, or legitimate interest for the processing of personal data.
- Personal data must only be used for specific purposes, kept accurate, and not be stored longer than needed.
- Parental consent is generally required for those under 16 years.

GDPR at a glance

Protects fundamental rights related to the processing of personal data

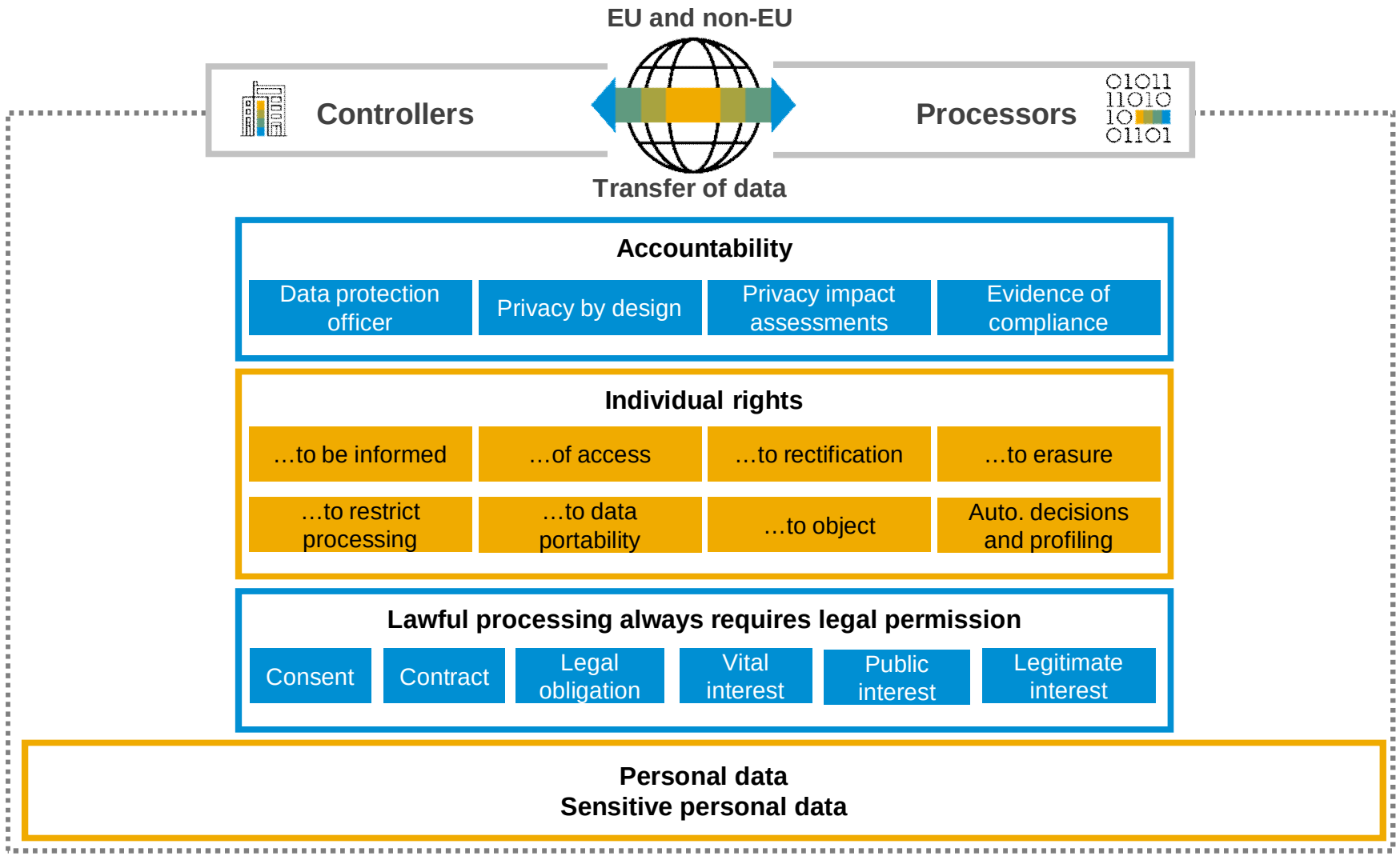


Individual rights

- GDPR recommends support of individual data requests through a self-service system where possible.
- Rights generally apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.

GDPR at a glance

Protects fundamental rights related to the processing of personal data

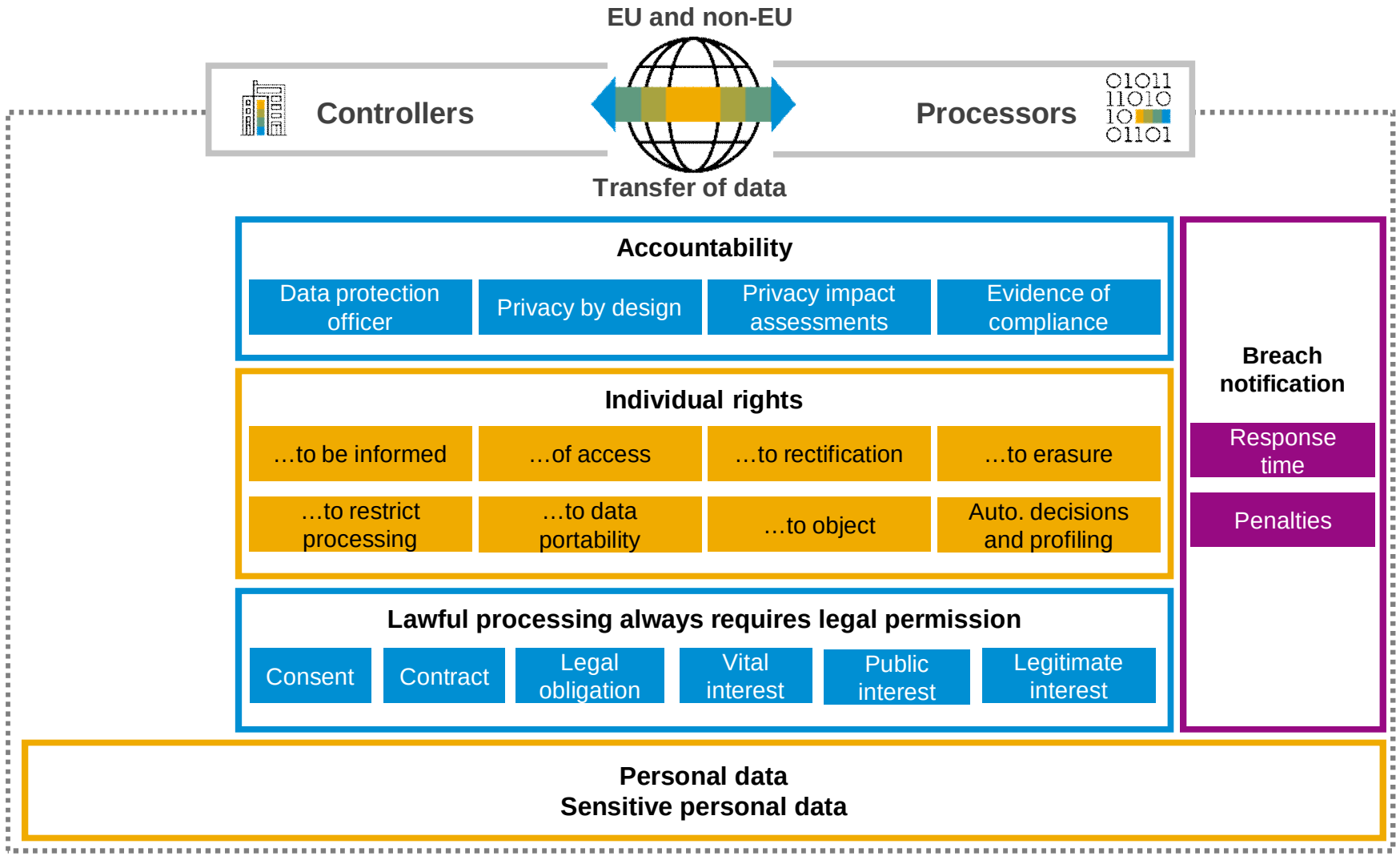


Accountability

- Involves a comprehensive framework and set of principles which allows (just as examples):
  - to produce and maintain evidence of actions to achieve and evaluate compliance
  - to assess data privacy risks and consider data protection in the early stages of product and project design
- Assign a DPO - Data Protection Officer – (companies with large-scale processing of personal data)

GDPR at a glance

Protects fundamental rights related to the processing of personal data

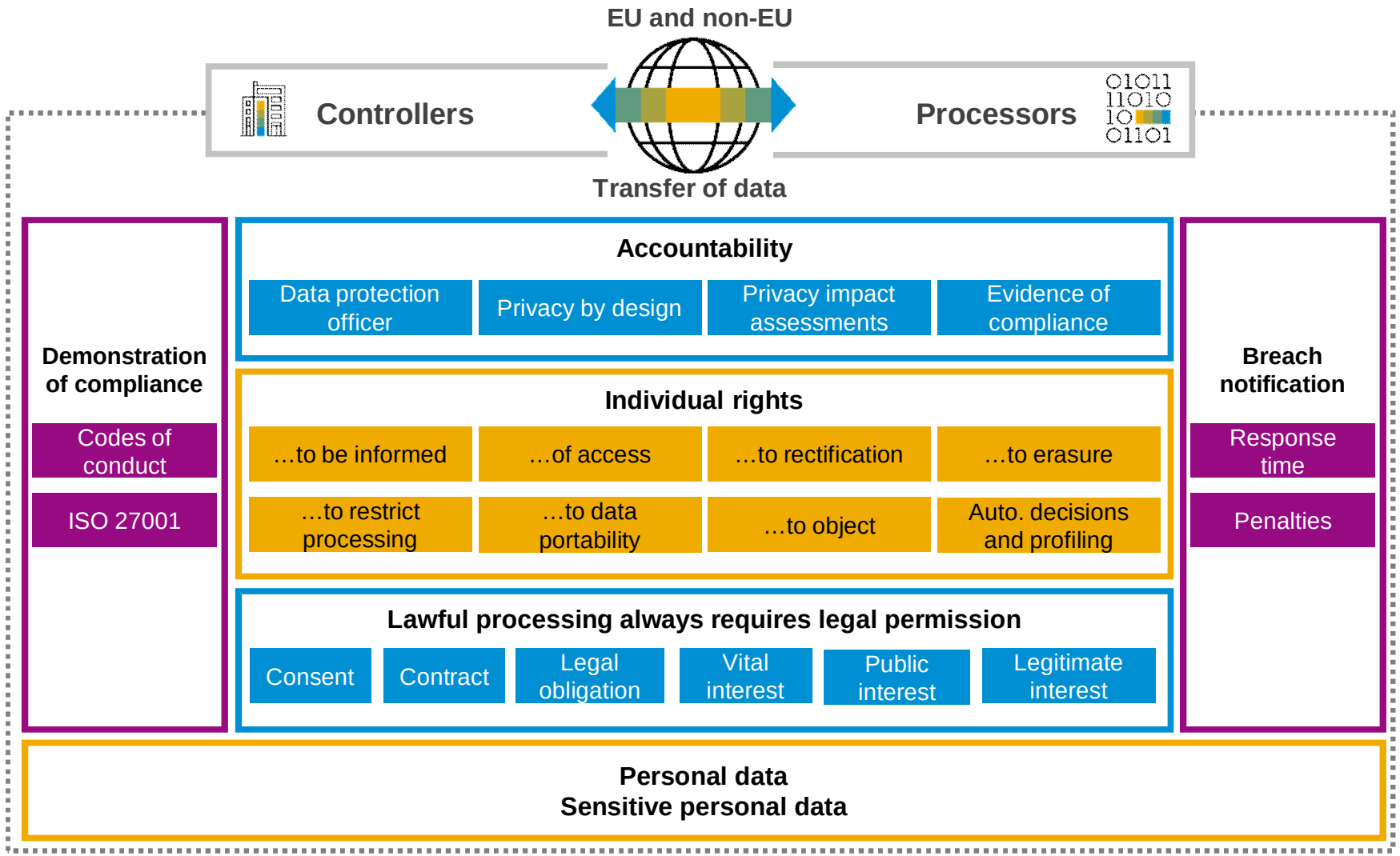


Breach notification

- Mandatory notification to supervisory authority within 72 hours of becoming aware of a personal data breach
- Communication to affected individuals without undue delay if breach is likely to result in high risk to rights and freedoms of individuals

GDPR at a glance

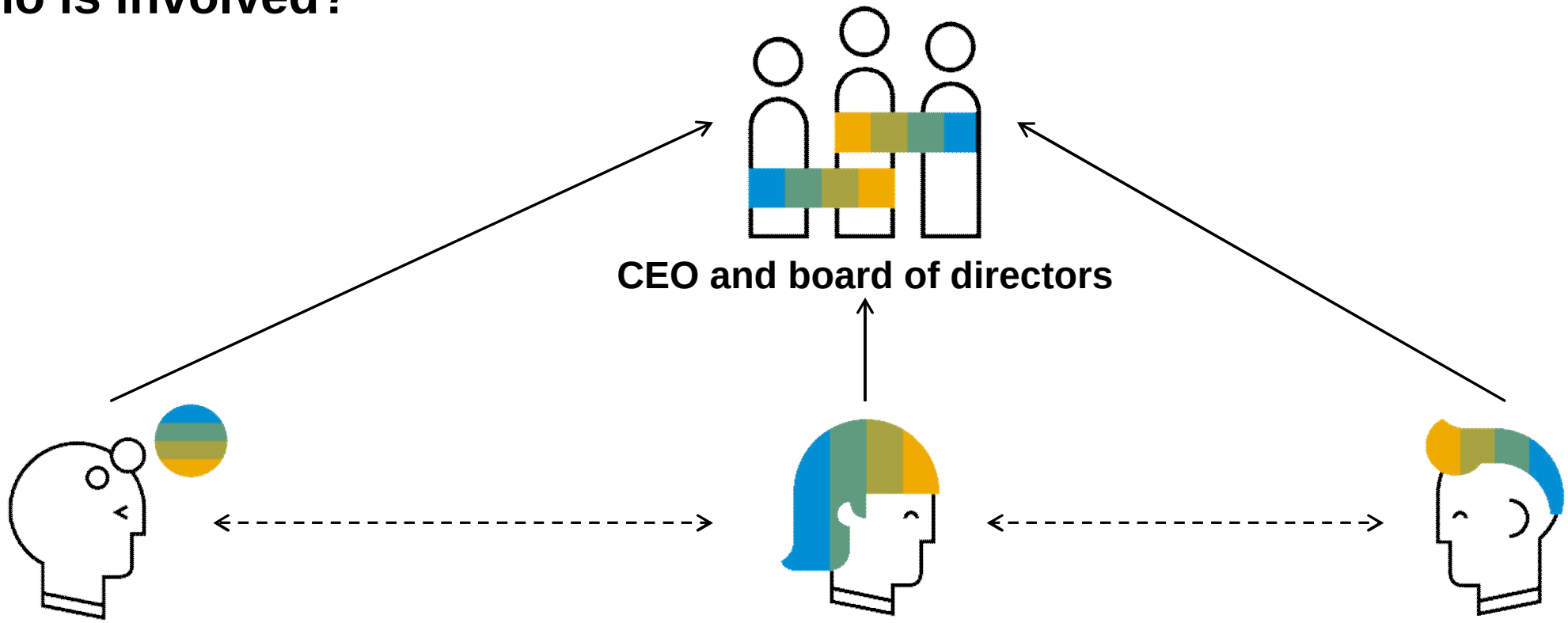
Protects fundamental rights related to the processing of personal data



Demonstration of compliance

- Compliance and accountability need to be an integral part of an overall data protection program.
- Communication of the codes of conduct, as well as privacy policies and procedures, help support compliance, with good understanding of data protection processes.
- Certifications will be a means to demonstrate compliance, but are not yet officially required or recognized.
- Other standards can also help show compliance, eg ISO 27001 (best-practice standard for information security, broader than GDPR).

Who is involved?



Governance

- Chief compliance officer
- Chief risk officer
- Head of legal
- Chief audit executive

Data protection officer

- Other data protection experts (chief data officer…)

Operations

- Chief information officer
- Chief information security officer
- Business process owners

Impact on your business

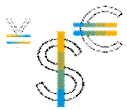
Challenges

Implementation effort is significant, broad, and complex

Initial effort to assess current status versus regulatory requirements and resulting gaps

Change management (organizational, policies, procedures, training, and communication…)

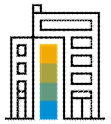
Prescribed data management: internal and external data, privacy by design, consent, storage, access, usage, retention, deletion



Sustainability and ongoing cost of the program—GDPR becomes “business as usual” once it becomes effective

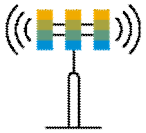
Opportunities

Better governance and data management improves business outcomes



Create strong framework and processes to mitigate risks and support compliance (for GDPR and others), with controlled costs

Improve depth and breadth of policies and procedures with clear accountability

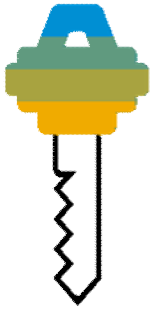


Embrace innovations like Big Data and the Internet of Things (IoT) with built-in data protection and privacy

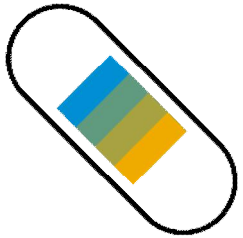
Improve confidence of business partners in the protection and security of their data, boosting business relations and your brand image

Business value of SAP solutions for GDPR

Keys to GDPR ROI

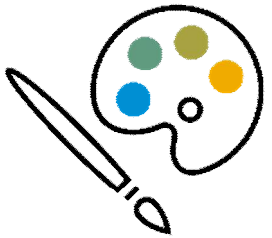


- Help avoid the large fines associated with GDPR
- Streamline and automate processes to help reduce compliance costs (*not* just for GDPR)
- Establish good data governance focused first on areas of highest risk
- Utilize existing SAP platform investments
- Access a consistent toolset with comprehensive capabilities for GDPR and beyond



Protect value

- Respect laws and regulations
- Reduce losses
- Improve governance and internal controls
- Reduce organizational and individual risk



Create value

- Improve overall management
- Release maintenance budget for development and innovation
- Enhance reputation and brand image
- Serve as a catalyst for digital transformation

Thank you.

Contact information:

F name L name
Title
Address
Phone number