
*Powering the trusted identities of the world's people, places & things*

# GDPR overview

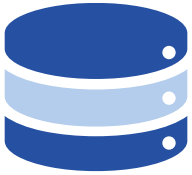
September 2017

# The GDPR: Scope

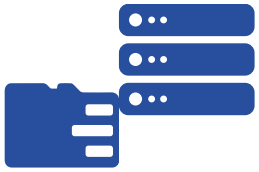
**GDPR takes effect May 2018!**

## It concerns:

Any information on an identifiable individual



In any data format (structured or unstructured)



On any support (online, offline, backup)

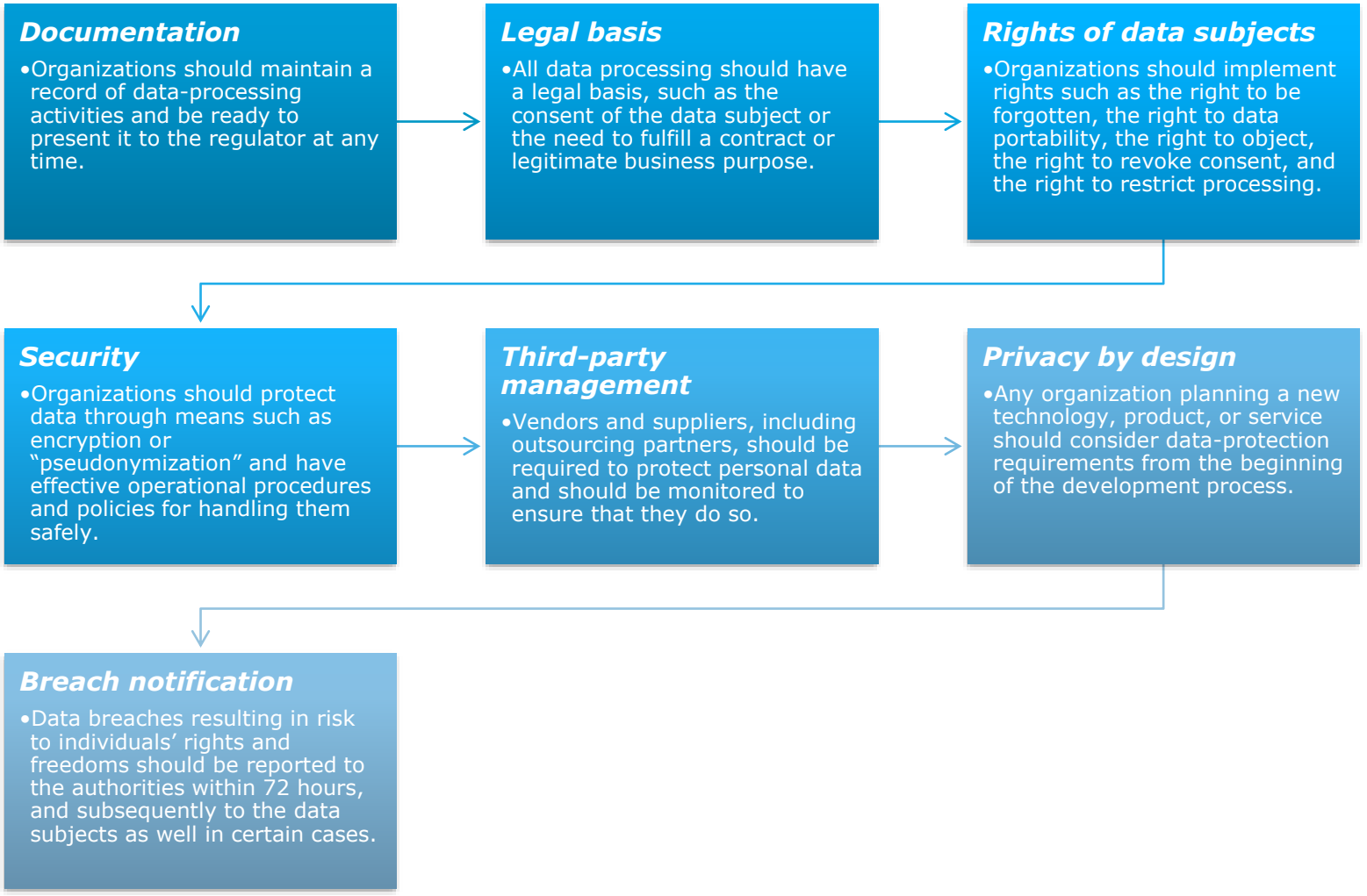
## It imposes:

Stringent consent requirement

Rights of the data subject

Obligation on organizations

# The GDPR: Requirements



# The GDPR: Enforcement

Individuals will be allowed to seek civil actions against organizations that violate their data-protection rights

It will be enforced via national supervisory authorities within the European Union

They will have the power to ban data processing

And give fines the highest between 20M€ and 4 percent of annual worldwide revenues

# The GDPR: guiding principles

## Lawfulness
- Data should be processed only when lawful

## Awarness
- The organizations should provide enough information on the users' right and the processing of the data

## Transparency
- The information provided to the users should be in a concise and understandable way

## Limitation
- Data may be collected and processed for an adequate, relevant and limited purpose only

## Accuracy
- Data should be accurate and kept up-to-date

## Storage
- Data should not be held in a format that permits personal identification any longer than necessary

## Security
- Data should be processed ensuring protection against theft, loss, damage and destruction

## Accountability
- The data controller is responsible for demonstrating compliancy

# What can HID bring for GDPR compliancy?

- Data controllers and processors "*shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk*" => *TDS*
- *"Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc."* => *MFA*
- *"Two-factor authentication should be considered for accessing mobile devices, and personal data stored at the mobile device should be encrypted"* => *MFA and Mobile Application Security*

Citations from Dec 16, ENISA's report (European Union Agency For Network and Information Security)

- High level security to protect data
- Authenticate the user to make sure it is the right user that is accessing the data
- Non-repudiated tamper evident audit logs to help the data controller demonstrating the compliancy

HID®

Powering
**Trusted Identities**


# Powering the trusted identities of the world's people, places & things