CSNP
CYBERSECURITY NON-PROFIT

# GDPR Compliance Guide

A practical guide for small to medium businesses and nonprofit organizations navigating EU data protection requirements

OVERVIEW

# Understanding GDPR

## What is GDPR?

The General Data Protection Regulation (GDPR) is the EU's comprehensive data protection law that came into effect on May 25, 2018. It strengthens privacy rights and imposes strict obligations on organizations that process personal data of EU residents.

## Core Objectives

- Protect individual privacy rights
- Harmonize data protection laws across EU
- Give individuals control over their data
- Increase accountability for organizations

# Does GDPR Apply to Your Organization?

### EU Establishment

Your organization has an office, branch, or subsidiary located in the European Union, regardless of where data processing occurs.

### EU Data Subjects

You offer goods or services to individuals in the EU, even if your organization is based outside Europe and transactions are free.

### Monitoring EU Residents

You monitor the behavior of individuals within the EU, including tracking online activity, profiling, or behavioral analysis.

If any of these apply, GDPR compliance is mandatory regardless of your organization's size or location.

FOUNDATION

# Seven Key GDPR Principles

01

## Lawfulness, Fairness & Transparency

Process data legally, fairly, and with clear communication to individuals

02

## Purpose Limitation

Collect data for specific, explicit, legitimate purposes only

03

## Data Minimization

Limit collection to what's necessary for your stated purposes

04

## Accuracy

Keep personal data accurate and up to date

05

## Storage Limitation

Retain data only as long as necessary

06

## Integrity & Confidentiality

Protect data with appropriate security measures

07

## Accountability

Demonstrate compliance and take responsibility

# Lawful Bases for Processing Personal Data

Under GDPR, you must identify at least one lawful basis before processing personal data. Choose the most appropriate basis for each processing activity:

### Consent

Individual freely gives specific, informed agreement for processing. Must be easy to withdraw.

### Contract

Processing is necessary to fulfill a contract with the individual or take pre-contractual steps.

### Legal Obligation

Processing is required to comply with laws and regulations applicable to your organization.

### Vital Interests

Processing protects someone's life or prevents serious harm in emergency situations.

### Public Task

Processing is necessary to perform official functions or tasks in the public interest.

### Legitimate Interests

Processing serves your legitimate interests, balanced against individual rights and freedoms.

INDIVIDUAL RIGHTS

# Data Subject Rights Under GDPR

### Right to be Informed

Clear information about data collection and use

### Right of Access

Request copies of their personal data

### Right to Rectification

Correct inaccurate or incomplete data

### Right to Erasure

Request deletion in certain circumstances

### Right to Restrict Processing

Limit how data is used temporarily

### Right to Data Portability

Receive and transfer data in machine-readable format

### Right to Object

Challenge processing based on legitimate interests

### Rights Related to Automated Decisions

Protection from solely automated decision-making

Organizations must respond to rights requests within one month, with the ability to extend by two additional months for complex requests.

# Privacy Notices: What to Include

1

## Controller Identity

Your organization's name and contact details, including your Data Protection Officer if applicable

2

## Processing Purposes

Why you're collecting the data and the lawful basis for each purpose

3

## Data Categories

Types of personal data you collect and process

4

## Recipients & Transfers

Who receives the data and any international transfers

5

## Retention Periods

How long data will be stored or criteria for determining retention

6

## Individual Rights

Clear explanation of rights and how to exercise them

RISK ASSESSMENT

# Data Protection Impact Assessments

## When Are DPIAs Required?

You must conduct a DPIA before processing that is likely to result in high risk to individuals' rights and freedoms. This typically includes:

- Systematic large-scale monitoring
- Large-scale processing of special categories of data
- Innovative use of new technologies
- Automated decision-making with legal effects
- Profiling with significant impacts

### Describe Processing

Document the nature, scope, context and purposes

### Assess Necessity

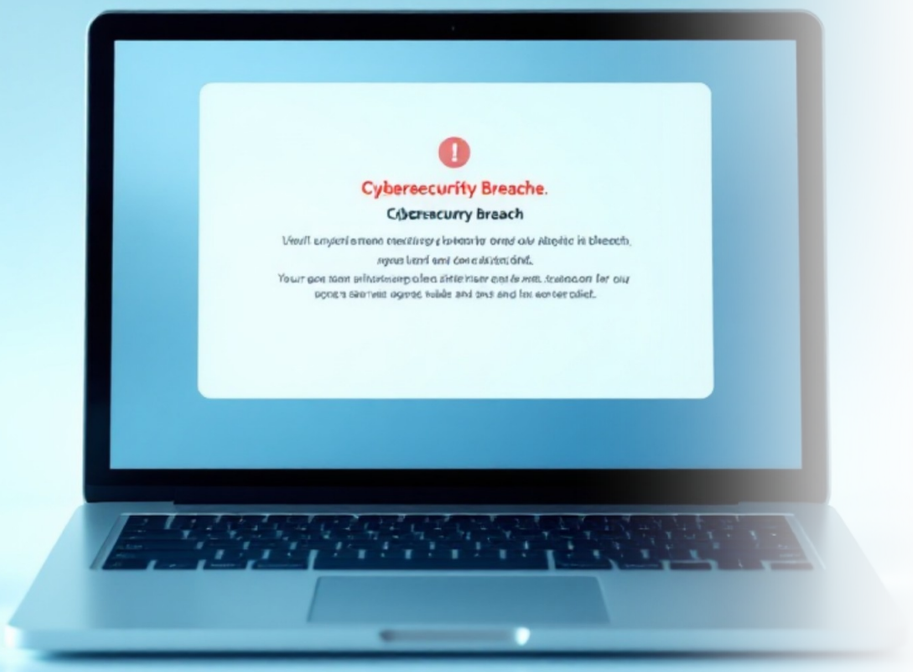
Evaluate necessity and proportionality

### Identify Risks

Determine risks to individual rights

### Implement Measures

Apply mitigation measures and safeguards




# Data Breach Notification Requirements

1

## Detection

Identify and assess the breach immediately upon discovery

2

## 72 Hours

Notify supervisory authority within 72 hours if risk to individuals

3

## Individual Notice

Inform affected individuals without undue delay if high risk

4

## Documentation

Record all breaches, including facts, effects, and remedial action

Not all breaches require notification to the supervisory authority, but all must be documented internally. Assess the risk to individuals' rights and freedoms to determine notification requirements.

# International Data Transfers

Transferring personal data outside the EU requires specific safeguards to ensure equivalent protection:

## Adequacy Decisions

Transfer to countries the EU Commission has deemed to provide adequate protection, including UK, Switzerland, and several others.

## Standard Contractual Clauses

Use EU-approved contract templates that guarantee appropriate data protection standards between parties.

## Binding Corporate Rules

Internal policies for multinational organizations approved by supervisory authorities for intra-group transfers.

## Certification Mechanisms

Approved certification schemes that demonstrate compliance with GDPR requirements for data protection.

DOCUMENTATION

# Essential Documentation Requirements

## Records of Processing Activities

Maintain detailed documentation including:

- Processing purposes and lawful bases
- Data categories and subject types
- Recipients and international transfers
- Retention schedules and security measures

## Additional Key Documents

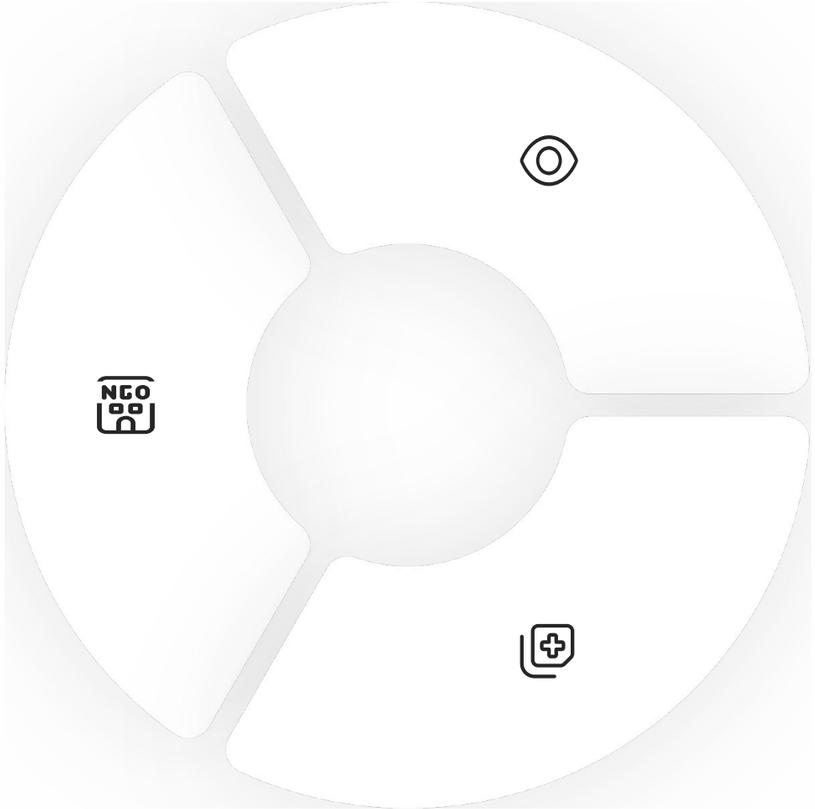
- Privacy notices and consent records
- Data protection impact assessments
- Breach notification logs
- Data processing agreements with vendors
- Training records and policies

Organizations with fewer than 250 employees have reduced documentation requirements, but must still document high-risk processing and special category data.

# Data Protection Officer Requirements

### Public Authority

Your organization is a public authority or body performing public tasks




### Large-Scale Monitoring

Core activities involve regular, systematic monitoring of individuals at scale

### Sensitive Data Processing

Core activities involve large-scale processing of special categories or criminal data

If any of these apply, you must appoint a Data Protection Officer who is independent, expert in data protection law, and adequately resourced. The DPO advises on compliance, monitors adherence, and serves as contact point for supervisory authorities and data subjects.

# Enforcement and Penalties

## €20M

### Maximum Fine

Or 4% of annual global turnover, whichever is higher

## €10M

### Lower Tier Fine

Or 2% of annual global turnover for certain violations

## Factors Affecting Penalties

- Nature, gravity, and duration of infringement
- Number of data subjects affected
- Degree of cooperation with authorities
- Previous infringements and compliance measures
- Level of technical and organizational measures

# GDPR Compliance Checklist

- **Data Mapping**

  Document all personal data processing activities

- **Lawful Basis**

  Identify and document lawful basis for each processing activity

- **Privacy Notices**

  Update and publish clear, comprehensive privacy notices

- **Consent Mechanisms**

  Review and update consent collection processes if applicable

- **Rights Procedures**

  Establish processes for handling data subject rights requests

- **Security Measures**

  Implement appropriate technical and organizational safeguards

- **Vendor Agreements**

  Review and update contracts with data processors

- **Breach Response**

  Develop data breach detection and notification procedures

- **Staff Training**

  Provide regular GDPR training to all employees

- **DPO Appointment**

  Appoint a Data Protection Officer if required

- **Documentation**

  Maintain records of processing activities and compliance measures

- **Regular Reviews**