Cybersecurity Considerations for GDPR

esentire®

What is the GDPR?

The General Data Protection Regulation (GDPR) is a brand new legislation containing updated requirements for how personal data of European Union (EU) citizens is handled. It was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. It is the result of years of preparation and debate, undergoing 4000 revisions.

There are two ways the EU legislates:

- ***Directives*** – these are passed down to member states and must be ratified by the national Parliaments before they come into effect. An example is the UK Data Protection Act (DPA) 1998, which is an implementation of EU Directive 95/46/EC. The UK DPA will be superseded by the GDPR.
- ***Regulations*** – these come into force without ratification and are applicable across all member states. This is the category under which the GDPR will fall.

When will it be enforced?

The GDPR will come into effect on May 25, 2018. As of this date, organizations in non-compliance will face heavy fines.

Who must adhere to the new regulation?

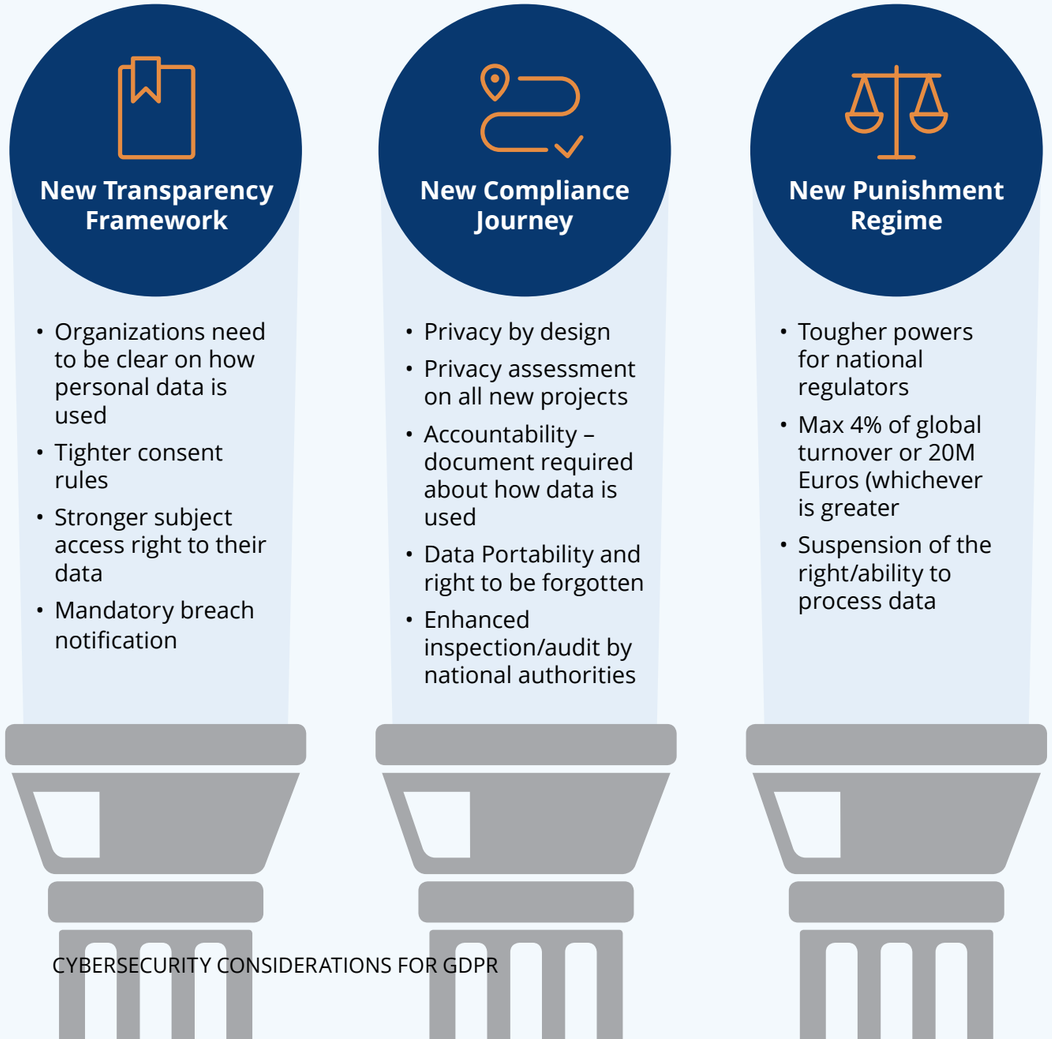
The regulation applies to all organizations that handle EU citizens' personal data, regardless of sector. This includes all enterprises, public sector entities and service providers that process their information. If you have responsibilities under the DPA, then you will certainly have to adhere to the GDPR.

Defined rules for Data Transfer outside the European Economic Area (EEA):

The transfer of subject data outside the EEA is allowed if the third country ensures an adequate level of protection due to its domestic law or the international commitments it's entered into. This extends to the following 11 countries:

ANDORRA	✓
ARGENTINA	✓
CANADA (COMMERCIAL ORGANIZATIONS)	✓
FAEROE ISLANDS	✓
GUERNSEY	✓
ISREAL	✓
ISLE OF MAN	✓
JERSEY	✓
NEW ZEALAND	✓
SWITZERLAND	✓
URUGUAY	✓

Summary of GDPR: Three Key Pillars



The GDPR and breach reporting

The GDPR will mean a number of big changes, but one of the most significant is the responsibility of organizations to report any breaches of personal data within **72 hours** of a determination of breach.

This is an important change, as no such duty of notification of breach has existed before.

Knowing this, organizations must ask themselves the following questions:

- How will I detect that I my infrastructure has been breached?
- Once I've detected a breach, how will I minimize the impact?
- How will I prove what happened?

What are the penalties of non-compliance?

There is a lot of scaremongering on this in the security industry. Unfortunately, until the GDPR comes unto effect, there is no way to know indefinitely how the fine regime will operate.

The GDPR states the following:

> ***"Fines under GDPR vary between 2-4% of the global turnover of the organisation or Euros 20 million (whichever is the greater) depending on severity of the infringement."*** [1]

In the worst case scenario, you may face a suspension of your right to trade.

1. https://www.eugdpr.org/key-changes.html

Regulations in detail

Article 4 Definitions: Personal data

For the purposes of this regulation, 'personal data' means any information relating to an identified or identifiable natural person ('data subject').[2]

Identifiable information can include a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

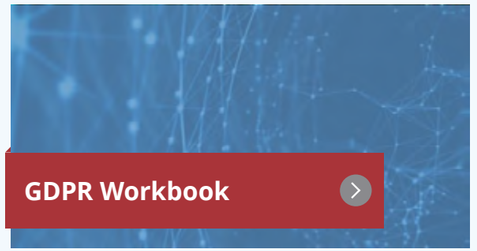
A 'personal data breach' therefore, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.[3]

Article 33 Definitions: Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the organization 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 competent in accordance with Article 55, 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 supervisory authority is not made within **72 hours**, it shall be accompanied by reasons for the delay.[4]

2. http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm
3. http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm
4. http://www.privacy-regulation.eu/en/article-33-notification-of-a-personal-data-breach-to-the-supervisory-authority-GDPR.htm

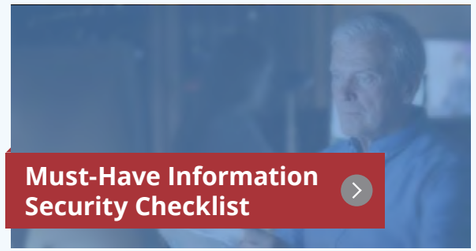
Resources to help prepare for the GDPR



The GDPR creates additional security and privacy obligations for organizations to comply with. All organizations, including those outside of the EU that hold data on European citizens, need to review their obligations under GDPR. Our GDPR workbook details the framework requirements, enabling you to map your current approach and gain an understanding of your areas of risk.

With this workbook, you will:

- Understand the key requirements of GDPR
- Determine how GDPR applies to your company
- Map your current approach to GDPR and evaluate your areas of risk



Regardless of industry, scope or scale, all businesses must employ a basic set of cybersecurity considerations to defend against today's growing cyber risk. This essential checklist provides high-level recommendations for basic cybersecurity assurance for easy adoption, implementation, and measurement.

This checklist will provide:

- Actionable measures to better defend your organization against cyber threats
- Recommendations to ensure the basic building blocks of a cybersecurity strategy are covered

eSentire Response Workbook | Preparing for the General Data Protection Regulation (GDPR)

REGULATION (EU) 2016/679 | General Data Protection Regulation
European Parliament / 27 April 2016

Based on the EU's recommendations, we've created this workbook to help align your company's cybersecurity practices with the expectations of the GDPR. Filling it out will serve as a gap analysis tool to identify what areas you need to focus on in the near-term as the GDPR approaches.

TOPIC		GDPR FRAMEWORK		DATA CONTROLLER PROFILE			ESENTIRE RECOMMENDATION		COST / EFFORT		CLIENT COMMENTS	
SEC	SUB	CATEGORY	DESCRIPTION	CURRENT	TARGETED	KEY ACTIVITY	PRIORITY	SERVICE	DAYS	BUDGET	NEXT STEPS	NOTES
01: GDPR AWARENESS												
01	A	GOVERNANCE	Board-level GDPR Awareness Training				Critical	Security Awareness Training				
01	B	GOVERNANCE	Operational (Executive) GDPR Awareness Training				Critical	Security Awareness Training				
01	C	GOVERNANCE	Employee GDPR Awareness Training				Critical	Security Awareness Training				
01	D	GOVERNANCE	Review Corporate Risk Register				Critical	Security Program Management				
01	E	GOVERNANCE	Identify and Record Compliance Violations/ Omissions/Risks				Critical	Security Gap Analysis				
02: DATA ACCOUNTABILITY												
02	A	COMPLIANCE	Document Personal Data: Type/Source/3P Organizations				Critical	Security Program Management				
02	B	COMPLIANCE	Identify Inaccurate Data				Critical	Security Gap Analysis				
02	C	COMPLIANCE	Share Updated Inaccurate Data with 3P Organizations				Critical	Security Gap Analysis				
02	D	COMPLIANCE	Develop GDPR Accountability Policies and Procedures				Critical	Security Policy Review and Creation				
03: COMMUNICATING PRIVACY POLICIES												
03	A	COMPLIANCE	Review Existing Privacy Notices				Critical	Security Policy Review and Creation				
03	B	COMPLIANCE	Document Legal Requirements				Critical	Security Policy Review and Creation				
03	C	COMPLIANCE	Document ICO Complaint Process				Critical	Security Policy Review and Creation				
03	D	COMPLIANCE	Identify GDPR Notice Requirements and Gaps				Critical	Security Policy Review and Creation				

TOPIC		GDPR FRAMEWORK		DATA CONTROLLER PROFILE			ESENTIRE RECOMMENDATION		COST / EFFORT		CLIENT COMMENTS	
SEC	SUB	CATEGORY	DESCRIPTION	CURRENT	TARGETED	KEY ACTIVITY	PRIORITY	SERVICE	DAYS	BUDGET	NEXT STEPS	NOTES
04: INDIVIDUAL RIGHTS MANAGEMENT												
04	A	COMPLIANCE	Procedures to Manage Subject Access				Critical	Security Policy Review and Creation				
04	B	COMPLIANCE	Procedures to Manage Inaccuracies Corrections				Critical	Security Policy Review and Creation				
04	C	COMPLIANCE	Procedures to Manage Information Erased				Critical	Security Policy Review and Creation				
04	D	COMPLIANCE	Procedures to Manage Direct Marketing				Critical	Security Policy Review and Creation				
04	E	COMPLIANCE	Procedures to Manage Automated Decision-Making/ Profiling				Critical	Security Policy Review and Creation				
04	F	COMPLIANCE	Procedures to Manage Data Portability				Critical	Security Policy Review and Creation				
05: SUBJECT ACCESS REQUESTS												
05	A	COMPLIANCE	Procedures to Manage Subject Requests (remove fees)				Critical	Security Policy Review and Creation				
05	B	COMPLIANCE	Procedures to Respond to SRs in 30 days (from 40)				Critical	Security Policy Review and Creation				
05	C	COMPLIANCE	Policies/Procedures to Refuse a Request				Critical	Security Policy Review and Creation				
05	D	COMPLIANCE	Documented Response to Subject Requests (cost/ benefit)				Critical	Security Program Management				
06: LEGAL BASIS FOR PROCESSING PERSONAL DATA												
06	A	COMPLIANCE	Document Legal Basis for Data Processing				Critical	Security Policy Review and Creation				
06	B	COMPLIANCE	Notification of Legal Basis of Data Processing (see 03:B)				Critical	Security Policy Review and Creation				

TOPIC		GDPR FRAMEWORK		DATA CONTROLLER PROFILE			ESENTIRE RECOMMENDATION		COST / EFFORT		CLIENT COMMENTS	
SEC	SUB	CATEGORY	DESCRIPTION	CURRENT	TARGETED	KEY ACTIVITY	PRIORITY	SERVICE	DAYS	BUDGET	NEXT STEPS	NOTES
07: CONSENT												
07	A	COMPLIANCE	Mechanism to Collect Consent				Critical	Security Policy Review and Creation				
07	B	COMPLIANCE	Mechanism to Collect Explicit Consent				Critical	Security Policy Review and Creation				
07	C	COMPLIANCE	Mechanism to Record and Report Consent				Critical	Security Program Management				
08: CHILDREN												
08	A	COMPLIANCE	Determine Local Definition of Child (eg: under 13)				Critical	Security Policy Review and Creation				
08	B	COMPLIANCE	Mechanism to Collect Parental/Guardian Consent				Critical	Security Policy Review and Creation				
08	C	COMPLIANCE	Mechanism to Record and Report Parental/Guardian Consent				Critical	Security Program Management				
09: DATA BREACHES												
09	A	BREACH RESPONSE	Documented Incident Response Plan				Critical	Incident Response Planning				
09	B	BREACH RESPONSE	Internal Process for Responding to an Incident				Critical	Incident Response Planning				
09	C	BREACH RESPONSE	Determined Goals of IR Plan				Critical	Incident Response Planning				
09	D	BREACH RESPONSE	Defined Roles and Responsibilities				Critical	Incident Response Planning				
09	E	BREACH RESPONSE	External and Internal Communication Strategy				Critical	Incident Response Planning				
09	F	BREACH RESPONSE	Remediation of Vulnerabilities in Systems				Critical	Incident Response Planning				
09	G	BREACH RESPONSE	Reporting of Incident and Remediation Activity				Critical	Incident Response Planning				
09	H	BREACH RESPONSE	Review of IR Plan following an Incident				Critical	Incident Response Planning				

TOPIC		GDPR FRAMEWORK		DATA CONTROLLER PROFILE			ESENTIRE RECOMMENDATION		COST / EFFORT		CLIENT COMMENTS	
SEC	SUB	CATEGORY	DESCRIPTION	CURRENT	TARGETED	KEY ACTIVITY	PRIORITY	SERVICE	DAYS	BUDGET	NEXT STEPS	NOTES
10: DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS (PIAs)												
10	A	COMPLIANCE	Conduct DPIA Assessment				Critical	Security Policy Review and Creation				
10	B	COMPLIANCE	Build Privacy by Design Policies and Procedures				Critical	Security Policy Review and Creation				
10	C	COMPLIANCE	High-Risk Systems DPIA Approval by ICO				Critical	Security Policy Review and Creation				
10	D	DETECTION	Aggregating and Correlating Data from Endpoint Sources				Critical	eMDR Detection and Response				
10	E	DETECTION	Aggregating and Correlating Data from Cloud Sources				Critical	Log Sentry				
10	F	DETECTION	Network Monitoring to Detect Cybersecurity Events				Critical	Managed Detection and Response				
10	G	DETECTION	Monitoring of Third-Party Activity				Critical	Managed Detection and Response				
10	H	DETECTION	Monitoring to Detect Unauthorized Users/Devices/ Software				Critical	Managed Detection and Response				
10	I	DETECTION	Evaluating Remote Requests to Identify Fraudulent Requests				Critical	Managed Detection and Response				
10	J	DETECTION	Software to Prevent Data Loss				Critical	Managed Detection and Response				
10	K	DETECTION	Penetration Testing and Vulnerability Scans				Critical	Enterprise Vulnerability Assessment				
10	L	DETECTION	Testing Event Detection Processes (Month/Year)				Critical	Security Awareness Training				
10	M	DETECTION	Analysis of Events to Improve Defensive Measures				Critical	Security Policy Review and Creation				
11: DATA PROTECTION OFFICER												
11	A	COMPLIANCE	Designated Data Protection Officer (DPO)				Critical	Security Policy Review and Creation				
11	B	COMPLIANCE	Designated Role and Budget for DPO				Critical	Security Policy Review and Creation				
12: INTERNATIONAL CONSIDERATIONS												
12	A	GOVERNANCE	Map International Operations (countries and offices)				Critical	Security Policy Review and Creation				
12	B	GOVERNANCE	Determine Governing Data Protection Supervisors				Critical	Security Policy Review and Creation				
12	C	GOVERNANCE	Document Investigation Lead and Process				Critical	Security Policy Review and Creation				

About eSentire

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real time to known and unknown threats before they become business disrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

For more information, visit **www.eSentire.com** and follow **@eSentire**.