General Data Protection Regulation (GDPR)

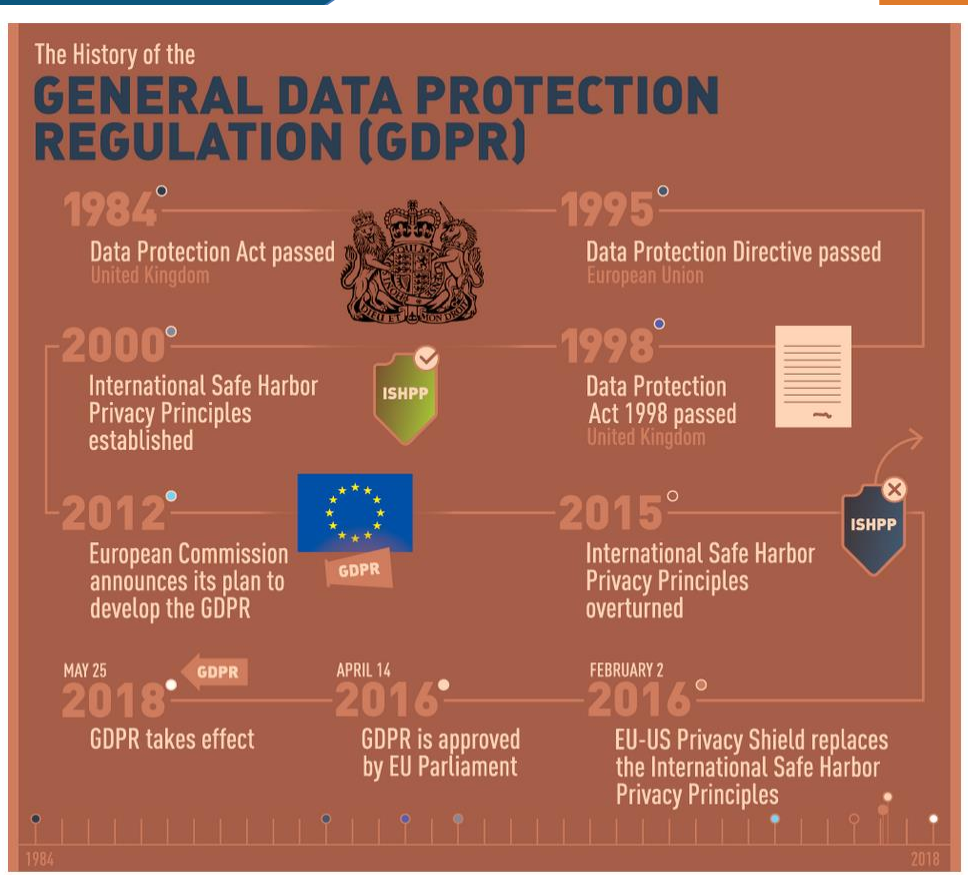
Jennifer Kurtz
Association for Continuity Professionals
15 June 2018

Manufacturer's EDGE

What is GDPR?

- GDPR is an expansion of the 1995 European Union Data Protection Initiative. Finalized in 2016, the deadline for compliance with GDPR was 25 May 2018.
- The GDPR introduces additional penalties, terminology, and information categories, thus providing broader compliance requirements than under the 1995 EU Data Directive.

Manufacturer's EDGE



A history of EU data protection regulations leading up to the GDPR.

Manufacturer's EDGE

How do privacy practices and expectations differ between the US and the EU?

USA	EUROPE
Underlying philosophy: right of expression; right to inform; right to privacy/right to be left alone (Louis Brandeis, 1890)	Underlying philosophy: right to be forgotten; right to erasure (essentially, right to delisting or delinking)
No uniform nationwide standard	EU minimum standard
50 different approaches (AL enacted data breach notification law 4 April 2018)	Possibility of country-by-country "add-ons"
Indefinite purpose/unlimited retention	Specific purpose/limited retention
Vermont: most aligned with GDPR as of early June with law passed requiring data brokers to register with the state, take standard security measures, and notify authorities of security breaches. Consumer rights to legal action if personal data used to discriminate.	Article 8 of the European Convention of Human Rights (ECHR) clearly specifies that "everyone has the right to respect for his private and family life, his home and his correspondence."
California: proposed California Consumer Privacy Act of 2018 would include GDPR-like consent option and redress for breaches	

Manufacturer's EDGE

Who should care about GDPR?

- GDPR addresses the rights and practices of different communities of data users that act with and within the European Union:
  - Data subjects (e.g., individuals whose characteristics or behaviors are being monitored)
  - Data controllers (those who possess sensitive data pertaining to data subjects, e.g., online retailer)
  - Data processors (those who work on behalf of the data controller, e.g., email automation service).
- https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

Manufacturer's EDGE

What are the underlying principles of the 1995 EU Data Protection Directive?

- Notice – individuals should be notified when their personal data is collected
- Purpose – use of personal data should be limited to the express purpose for which it was collected
- Consent – individual consent should be required before personal data is shared with other parties
- Security – collected data should be secured against abuse or compromise
- Disclosure – data collectors should inform individuals when their personal data is being collected
- Access – individuals should have the ability to access their personal data and correct any inaccuracies
- Accountability – individuals should have a means to hold data collectors accountable to the previous six principles

Manufacturer's EDGE

GDPR Principles

Transparency
controllers provide much more detailed information about how data are processed, what grounds are being used to justify fair processing and what rights individuals have to access, delete and port data, and object to processing.

Data Minimalization
A new principle requiring the level and type of data being processed in each case to be limited to the minimum necessary.

Manufacturer's EDGE

Key Changes

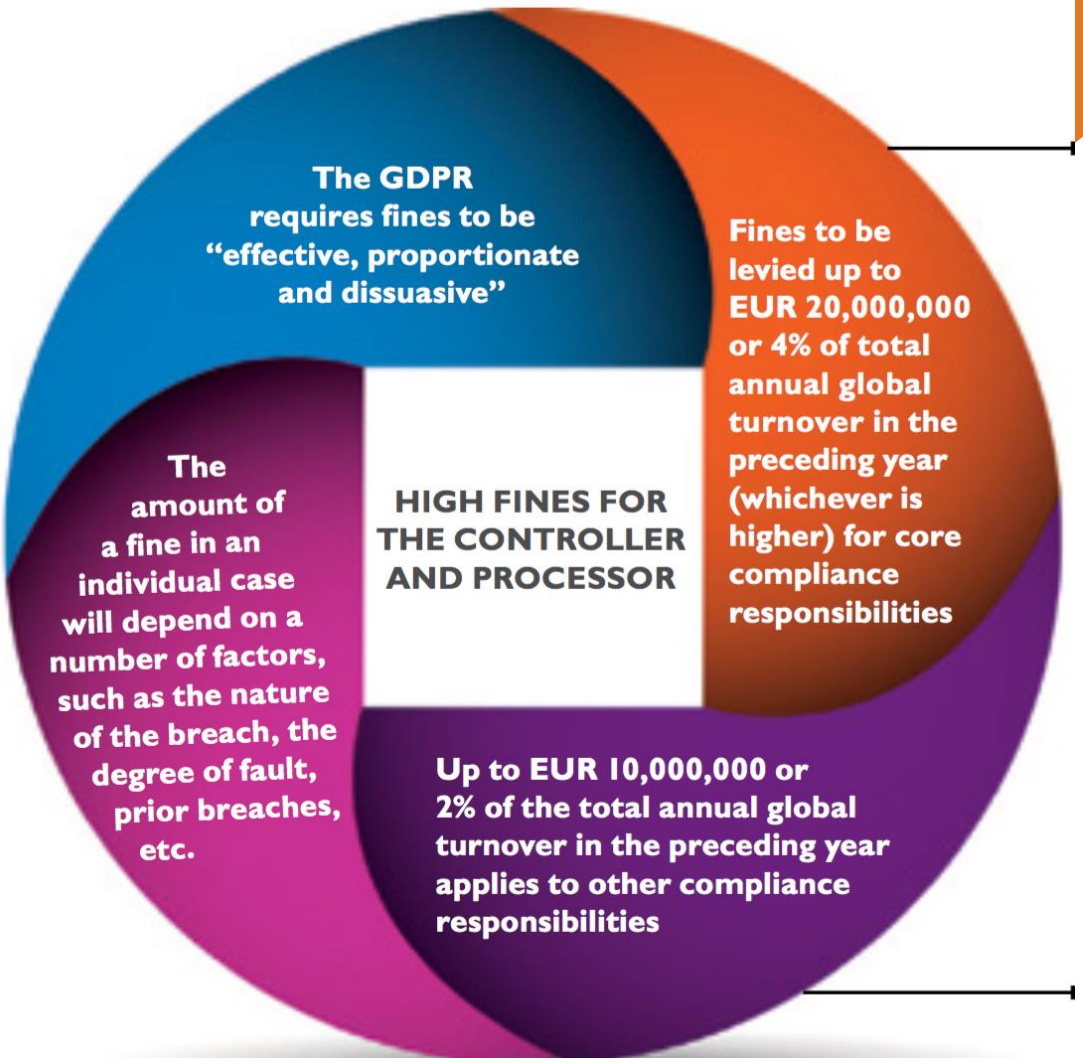
- Expansion of sensitive information to include digital and location identifiers, as well as biometrics
- Requirement to apply principles of ‘privacy by design’ and ‘privacy by default’ into the process of developing and launching new technologies, products, services, etc.
- New obligation to carry out privacy impact assessments
- New rights to data portability and a right to be forgotten
  - Time limits for subject access requests
- New requirement to notify data protection supervisory authorities if a data breach takes place (within 72 hours)
- Fines for non-compliance of up to EUR 20,000,000 or (if higher) 4% of the global annual turnover of the organization
- Special rules around profiling and use of children’s data

Manufacturer's EDGE

Penalties

- Regulatory
  - Up to EUR 20,000,000 or
  - Up to 4% of annual worldwide revenues for previous years
  - Whichever is greater
- Compensation claims
  - From data controller or processor for damage suffered
  - Violation of local laws (providing criminal sanctions for GDPR breach)
  - May be made by not-for-profit bodies, associations, organizations on behalf of data subjects

Manufacturer's EDGE



Manufacturer's EDGE

Terminology

- Basic definitions of “processing”, “filing system”, “controller”, and “processor” are largely as in the Directive
- Definition of “personal data” is also as in the Directive, but is supplemented to clarify that location data and online identifiers (e.g., IP addresses) also constitute personal data
- Many new definitions have been introduced, such as “profiling”, “personal data breach”, “pseudonymization”, “biometric data”, “data concerning health”, “group of undertakings”, and “cross-border processing”

Manufacturer's EDGE

“Sensitive Data” Expansion

- **Biometric data** – means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
- New detailed rules regarding situations where data are used to undertake automated decisions impacting individuals (profiling)
- **Profiling** – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Manufacturer’s EDGE

Slightly Modified

- Organizations from outside the EU, in relation to the offering of goods (and services) to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.
- All entities to which the GDPR will apply should conduct an analysis of the impact of the GDPR on their business activities
- Non-EU based entities should make strategic decisions on their approach to the requirements of the Regulation and designate a representative for the EU for the purposes of the Regulation. (For more information see “Representative of the controller within the EU”)

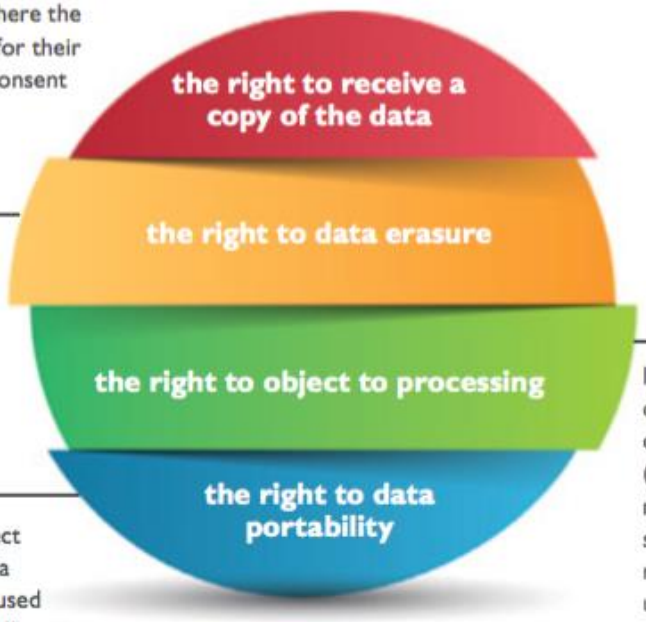
Manufacturer's EDGE

What are important things for my US-based organization to consider with respect to GDPR compliance?

- What data do we collect about EU citizens?
- Why do we collect the data?
- How do we protect the data?
- Who processes it on our behalf?
- With whom do we share the data?
- What is the process for a data subject to learn what data has been collected?
- How do we track the disposition of the data?
- How do we detect misuse of the data?
- What is the notification process to data subjects?

Manufacturer's EDGE

The data may require the controller to erase personal data on request in a range of scenarios – e.g. where the data are no longer required for their original purpose, or where consent to processing has been withdrawn.



This right allows a data subject to receive their personal data "in a structured, commonly used and machine-readable format" and to transmit data in that format to another controller.

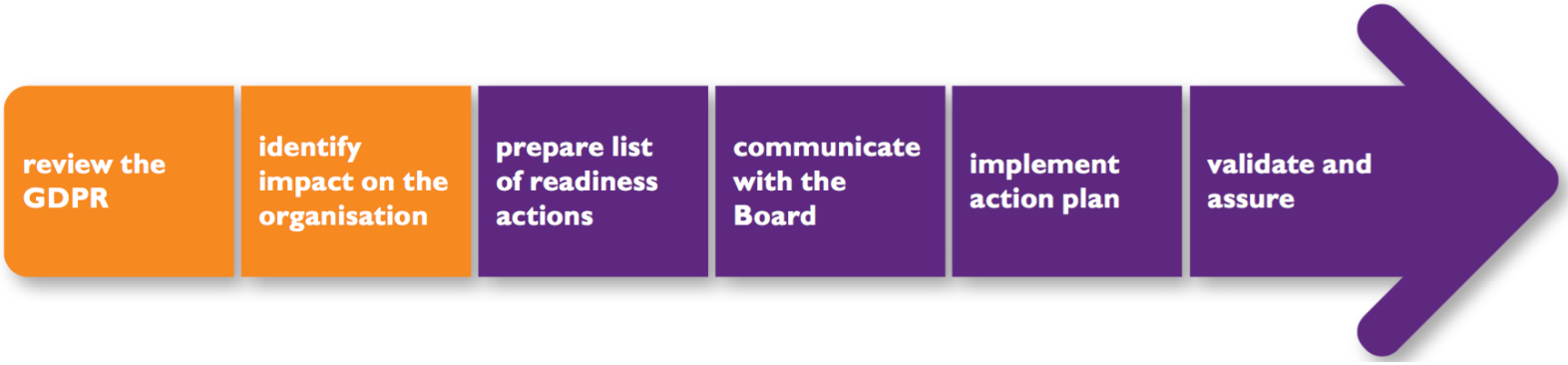
Individuals have the right to object to processing based on legitimate interests (including profiling), direct marketing, research and statistics. If exercised, this request must be respected unless the organisation can show there are compelling grounds to continue with the processing which overrides the individual's rights, or if the processing is required to establish, exercise or defend legal claims.

Sector-Specific/Location-Specific

- Monitor emerging codes of conduct relevant to the particular sectors in which your business operates
- Assess the impact of those codes of conduct on your business activities
- Understand how the changes made to key definitions impact your processing activities
- Check for additional provisions enacted at the country level (e.g., France, Germany)

Manufacturer's EDGE

Next Steps



Source: DLA Piper – A Guide to the General Data Protection Regulation (p. 9)

Manufacturer's EDGE

Current State: GDPR Relevance

- Determine whether company is data controller or data processor
- Map dataflows
- Capture data record attributes
- Maintain records of processing activities
- Define event versus incident

Manufacturer's EDGE

Principle of Accountability

- Data controller displays active compliance through integrated data protection throughout processes and culture
- Say what you do: integrate data protection in processes and culture
- Show what you do: maintain clear records of all data operations
- Do what you say: use mechanisms/procedures for monitoring/verifying
  - Train your people
  - Build in ”privacy by design” from the git-go
  - Perform a privacy risk assessment (PIA) on new projects/processes
  - Build in “privacy by default”
  - Appoint a DPO if needed (usually public entity processing personal data or large scale monitor/processor)

Manufacturer's EDGE

US-Based Data Controllers

- Designate a representative in the EU to interact with local supervisory authorities unless
  - Processing is occasional
  - Processing of sensitive data is not involved
- Follow eight key steps for Privacy Shield compliance
  - Yuli Takatsuki (25 July 2016), A Practical Guide to the EU-US Privacy Shield, https://privacylawblog.fieldfisher.com/2016/a-practical-guide-to-the-eu-us-privacy-shield
  - Webinar <https://www.youtube.com/watch?v=XDkF4gqozEc&feature=youtu.be>

Manufacturer's EDGE

Supply Chain, Teams, Partnerships

- Define data privacy-related roles and responsibilities with processors
- Include contractual provisions
- Designate a POC for data subjects
- Provide clear descriptions of data uses
- Joint and several responsibility (and liability) enforced via GDPR for controllers and processors
  - Big expansion from the 1995 Directive
  - Review and as needed revise agreements with data processors
  - Update related tendering documents and processes (e.g., RFP documentation, specimen letters and agreements to be used in procurement procedures)
- Requires data processing agreement (data breach, erasure upon service completion, cooperation with data controller)

Manufacturer's EDGE

Traditional Incident Response

- Event occurs
- Alert
- Event analysis (ticket is created if policy violated; availability versus confidentiality or security issue—need to understand JK)
- Response
  - Start documentation
  - Incident type (i.e., CIA)
  - Assemble team
  - Assess for impact
  - Determine notification requirements
- Debrief

Manufacturer's EDGE

Future State: Certification

- Keep an eye out for certification marks that become available and assess the organization's eligibility to apply for certification
- Implement procedures to ensure that the adopted solutions comply with the requirements of the GDPR
- May also support transfers to a third party

Manufacturer's EDGE

Lessons Learned from Ping Identity

- Log files
- Incident type CIA
- PII type/encryption
- Controller/processor
- Severity
- Notification
- Data breach register
- Updates to policy
- Process/control revisions
- Privacy by design (core GDPR tenet) and SDLC

Manufacturer's EDGE

Next Steps

- Focus on detection: more data/logging; evidence that something happened
- Collect data: most valuable log data and retention; integrity; SIEM/IDS; What can you prove?
- Be prepared: set a goal; measure gap; create plan; cross-functional; practice and use; open environment to share info; review contract negotiations and timing reqs; prenegotiate service agreements with forensic services
- Perform high-level survey to receive your Data Privacy Score at https://www.dlapiperdataprotection.com/scorebox/index.html

Manufacturer's EDGE

Privacy Shield Compliance: Eight Key Steps

1. Update your privacy policies
2. Provide users with means of opting out / opting in
3. Revisit your third-party contracts
4. Pick your independent recourse mechanism
5. Get your internal policies in order
6. Set up procedures for annual assessments and re-certifications
7. HR data - further steps
8. You're ready to self-certify! <https://www.export.gov/article?id=Self-Certification-Information>

Manufacturer's EDGE

QUESTIONS?

jkurtz@manufacturersedge.com

Manufacturer's EDGE