European Union
General Data Protection Regulation and it's Potential Impact

EU – GDPR

EU General Data Protection Regulation

- GDPR was approved and adopted by the EU Parliament on April 14th, 2016 and enforced on May 25th, 2018
  - Organizations within the EU had a 2 year transition period
- The GDPR has the objective to protect the personal data of anyone in the EU. GDPR provides the legal framework to make Personal Data collection and processing lawful, fair, and transparent.
  - GDPR applies to EU citizens or others that live, work, or travel through the EU
  - GDPR applies to organizations outside the EU if they sell goods or services, or offer them for free to individuals in the EU or if they monitor the behavior of individuals in the EU

General Data Protection Regulation Overview

- The scope of the GDPR is extensive for this presentation the focus will be on the following key highlights:
  - Enhanced Rights
  - Fines and Penalties
  - Breach Notifications
  - Data Processors in Scope
  - Data Protection Officers
- GDPR Stakeholders
  - **Data Subject**, a natural person
  - **Data Controller**, a natural or legal person, public authority, or organization that collects data from a DS
  - **Data Processor**, a natural or legal person, public authority, or organization that processes data on behalf of the DC

Examples of what is Considered Personal Data

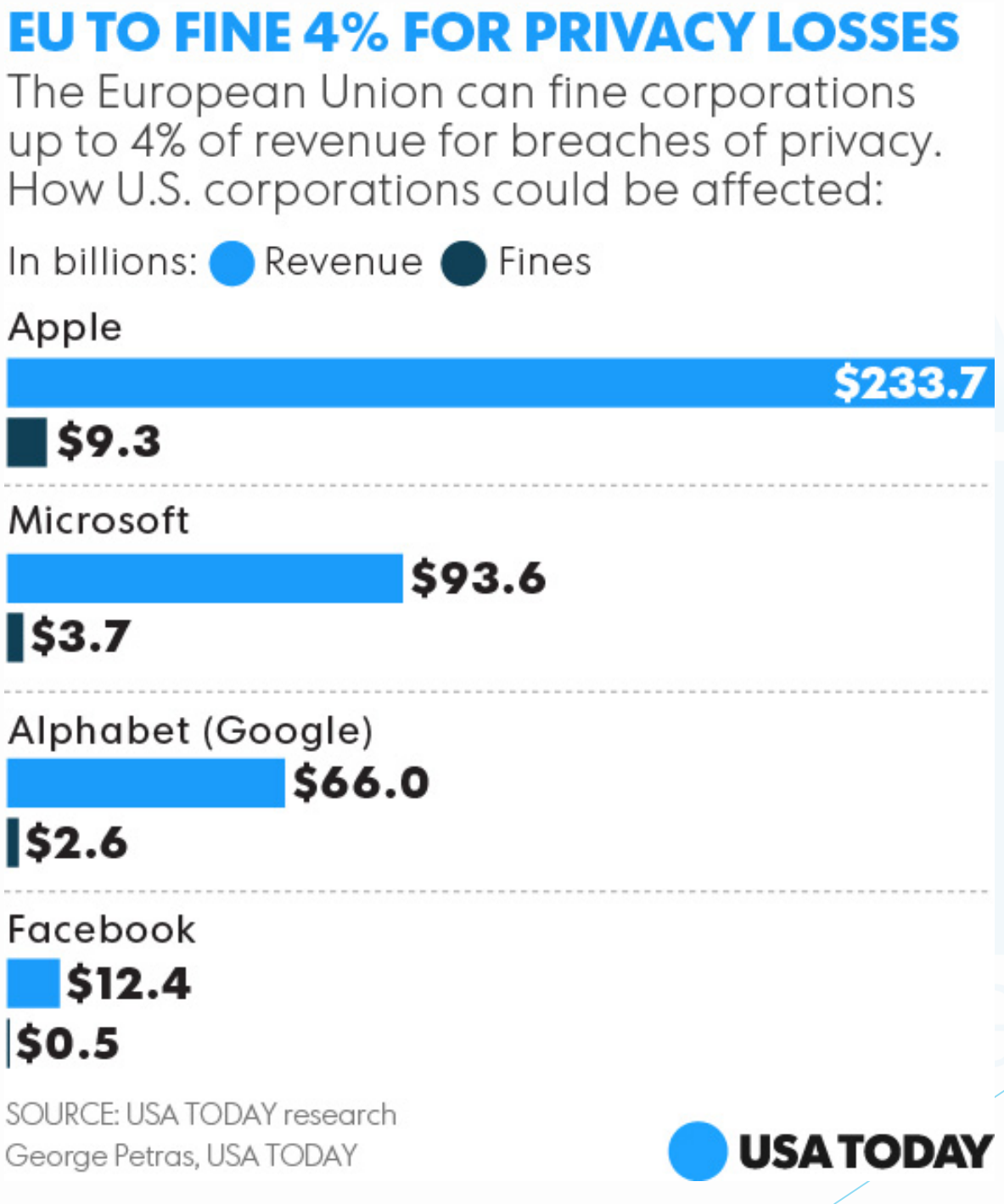
- Personal Data
  - Name
  - Address
  - Email address
  - Photo
  - IP address
  - Location data
  - Online behavior (cookies)
  - Profiling and analytics data
- Special Category of Personal Data
  - Race
  - Religion
  - Political opinions
  - Trade union membership
  - Sexual orientation
  - Health information
  - Biometric data
  - Genetic data

Enhanced Rights

- With the introduction of the GDPR the Data Subject (DS) gets greater rights than before.
- GDPR is about empowering the individual. The DS has more control over the USAGE, RETENTION, and MOVEMENT of their personal data. The data subject rights now include but are not limited to the following:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure or the right to be forgotten
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - The right not to be subject to automated decision-making including profiling
  - The right to consent

Fines and Penalties

- The GDPR imposes stiff fines and penalties on those that collect and process the Personal Data of EU based data subject if the organizations are not in compliance. The fines and penalties are stiff because they are meant to be dissuasive.
- The fines are administrated by the Data Protection Authority (DPA) in the individual EU member states. In the Netherlands the “Autoriteit Personsgegevens” is the DPA. The following criteria are used to determine the weight of the fines in case a organization is non-compliant
  - Nature of the infringement, Intention, Mitigation, Preventative measures, History, Cooperation, Data type, Notification, and Certification
  - The administrative fines imposed could be up to 20 million Euros or 4% of the global annual revenue of the prior financial year, whichever is higher
- The GDPR also includes a provision giving persons the right to bring individual or collective legal action against non-compliant entities. Under the GDPR data subjects may seek compensation for “material or non-material” damages from any entity that processed their personal data in violation of the GDPR.
- Damage to an organizations reputation could be costly.


EU TO FINE 4% FOR PRIVACY LOSSES
The European Union can fine corporations up to 4% of revenue for breaches of privacy. How U.S. corporations could be affected:
In billions: Revenue Fines
Apple
$233.7
$9.3
Microsoft
$93.6
$3.7
Alphabet (Google)
$66.0
$2.6
Facebook
$12.4
$0.5
SOURCE: USA TODAY research
George Petras, USA TODAY
USA TODAY

Breach Notifications

- In the case there is a breach of personal data, the controller must without undue delay and, where feasible, report the incident to the DPA, not later than 72 after becoming aware of the breach. If the controller is not able to notify the DPA within 72 hours of a breach, the late notification must be accompanied by reasons for the delay.
- The indicated notification to the DPA must contain the following:
  - A description of the nature of the breach
  - A approximation of the number of data subjects concerned
  - A approximation of the number of personal data records concerned
  - Contact info for the DPO
  - Likely consequence of the data breach
  - Steps taken or proposed by the controller to address the data breach
- It is the responsibility of the controller to provide proper documentation of any data breach, the documentation must enable the DPA to verify the organizations level of compliance

Data Processor in Scope

- The Data Processor (DP) is a natural or legal person, public authority, or organization that has the contractual obligation to analyze/process the data collected from the Data Subject (DS) on behalf of the Data Collector (DC) for the specific purpose of delivering goods and services.
- The DC and DP have many equal duties and will have to adhere to similar principles under GDPR. The DP shall provide sufficient guarantees that it is capable of implementing appropriate technical and organizational measures to the extent that the DP will meet or exceed the requirements as outlined under GDPR.
- The DP has the obligation to assist the DC in it's reporting in case of a data breach
- Under GDPR the DC and DP that collect and process the personal data of a DS never own the personal data. The personal data will always be the property of the natural person

Data Protection Officer

- In certain circumstances data controllers and processors must designate a Data Protection Officer (the DPO)
  - processing is carried out by a public authority
  - the core activities of the controller or processor consist of processing which, by its nature, scope or purposes, requires regular and systematic monitoring of data subjects on a large scale
  - the core activities consist of processing on a large scale of special categories of data

The Principles that apply to Personal Data Collection and Processing under GDPR

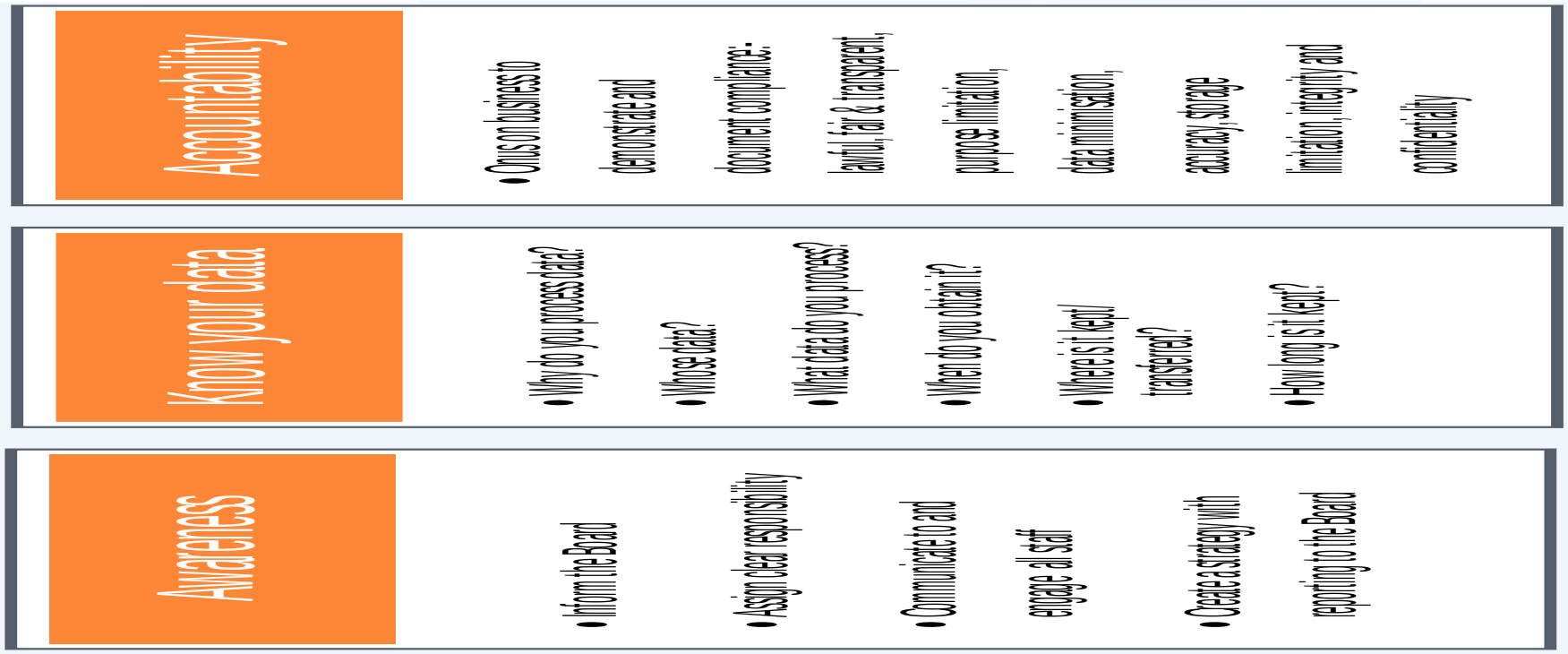
- Personal Data must be collected lawfully, fairly, and transparently
- Personal Data can only be collected for specified, explicit, legitimate purposes
- Personal Data must be adequate, relevant, and limited to what is necessary for processing
- Personal Data must be accurate and kept up to date
- Personal Data must be kept in a form such that the data subject can be identified only as long as is necessary for processing
- Personal Data must be processed in a manner that insures its security

The Data Controller (DC) has the responsibility to comply with the above principles. The DC also is responsible to ensure that any external Data Processer it contracts complies with the same principles.

GDPR Compliance Starts with Mapping collected Data

- Mapping the 5 W's
- Why does your organization process personal data?
- Whose personal data is process by your organization?
- What type of personal data is processed by your organization?
- When does your organization obtain the personal data?
- Where is the personal data kept/transferred by your organization?

10 Things that Organizations need to Know and Do as it related to GDPR
3 0f 10



10 Things that Organizations need to Know and Do as it related to GDPR
6 0f 10

Consent

- New rules for obtaining and withdrawing consent
- Additional rules for children
- Clear plain language
- Tangible evidence of consent

Transparency

- Inform Data Subjects:-
  - who you are;
  - why you process data;
  - what you will do with it;
  - how long will you keep it.
- Advise them of their rights and how to exercise them.

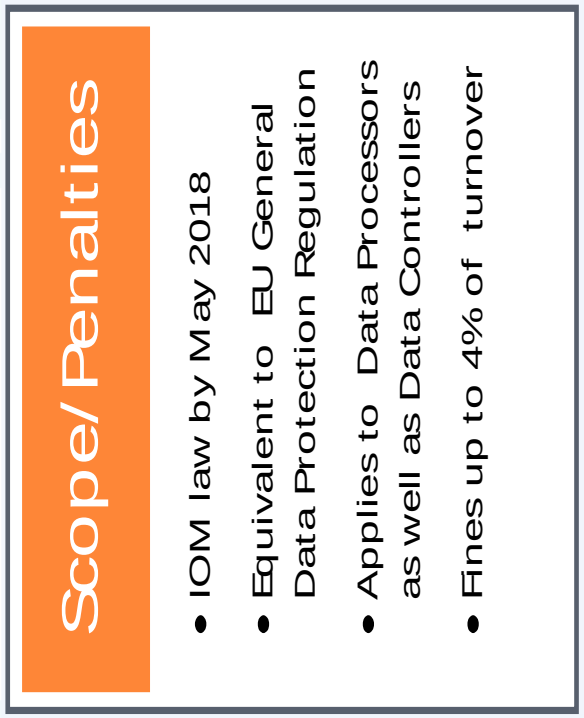
Security

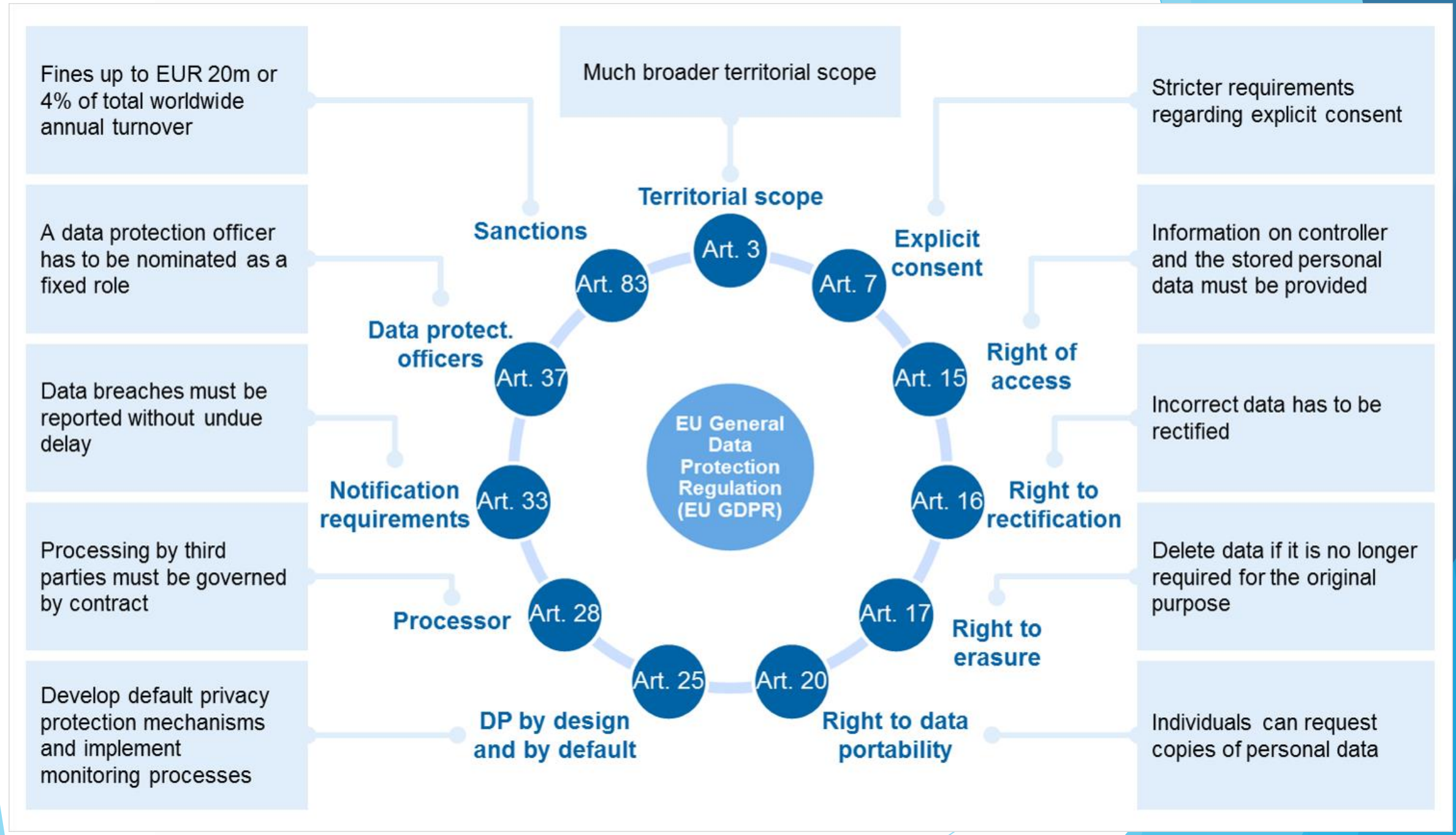
- Adopt measures to ensure ongoing confidentiality, integrity, availability and resilience
- Ability to restore timely access after incident
- Regularly tested

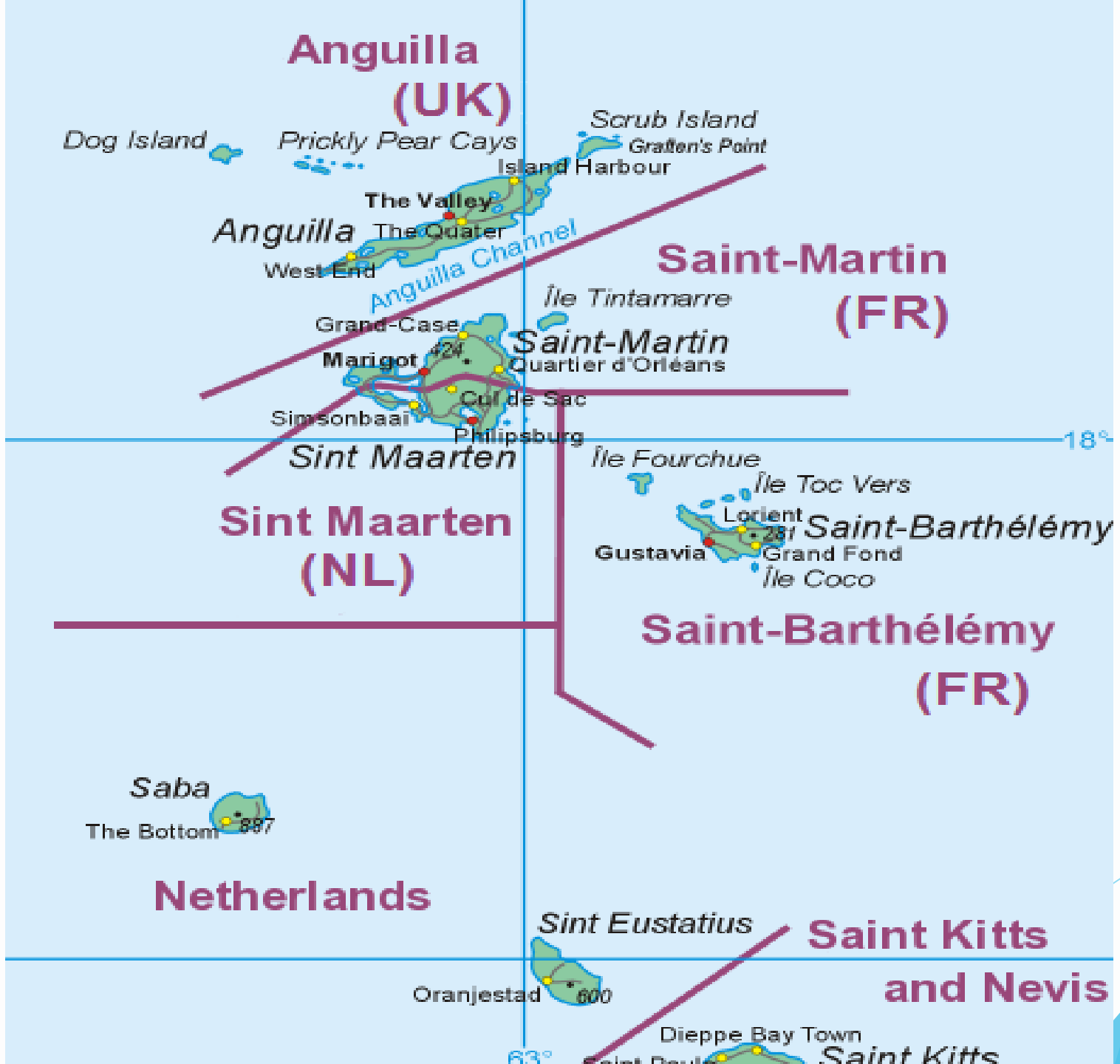
10 Things that Organizations need to Know and Do as it related to GDPR
9 0f 10

Rights	• New and enhanced • Free to exercise with reduced compliance time • Right to object data portability & more
Privacy by Design/DPIAS	• DP requirements • designed in to any new project from outset • Mandatory DPIA part assessments and prior authorization • Involve DPO
Data Protection Officers (DPO)	• If required appoint a DPO with knowledge • Reports to highest level of management • Cannot be instructed • Duties cannot conflict

10 Things that Organizations need to Know and Do as it related to GDPR
10 0f 10




Fines up to EUR 20m or 4% of total worldwide annual turnover
Much broader territorial scope
Stricter requirements regarding explicit consent
A data protection officer has to be nominated as a fixed role
Information on controller and the stored personal data must be provided
Data breaches must be reported without undue delay
Incorrect data has to be rectified
Processing by third parties must be governed by contract
Delete data if it is no longer required for the original purpose
Develop default privacy protection mechanisms and implement monitoring processes
Individuals can request copies of personal data
Sanctions
Art. 83
Territorial scope
Art. 3
Explicit consent
Art. 7
Data protect. officers
Art. 37
Right of access
Art. 15
EU General Data Protection Regulation (EU GDPR)
Notification requirements
Art. 33
Art. 16
Right to rectification
Processor
Art. 28
Art. 17
Right to erasure
Art. 25
Art. 20
DP by design and by default
Right to data portability


Anguilla
(UK)
Dog Island
Prickly Pear Cays
Scrub Island
Crocus Bay
Island Harbour
The Valley
Anguilla
The Quarter
West End
Anguilla Channel
Saint-Martin
(FR)
Île Tintamarre
Grand-Case
Saint-Martin
Marigot
Quartier d'Orléans
Cul de Sac
Simsonbaai
Philipsburg
Sint Maarten
18°
Île Fourchue
Île Toc Vers
Lorient
Saint-Barthélémy
Gustavia
Grand Fond
Île Coco
Sint Maarten
(NL)
Saint-Barthélémy
(FR)
Saba
The Bottom
887
Netherlands
Sint Eustatius
Saint Kitts
and Nevis
Oranjestad
600
Dieppe Bay Town
63°
Saint Kitts

St. Maarten and GDPR

- GDPR does not apply to St. Maarten. St. Maarten has its own National Ordinance Personal Data Protection (20-12-2010, AB 2010, GT no. 2). St. Maarten is to instate its own Data Protection Supervisory Committee. The committee will have the responsibility to enforce the national ordinance.
- St. Maarten is geographically between St. Martin and St. Barth both are an integral part of France which is on of the 28 EU member states. GDPR applies to St. Martin and St. Barth.
- GDPR does not apply to Saba and St. Eustatius, at least not as of May 25th, 2018. Until further notice the Data Privacy Law, will remain valid but additional condition may apply considering that sensitive information is shared between BES and EU entities. This may impact business between St. Maarten and Saba / St. Eustatius
- Is the St. Maarten Immigration Form GDPR compliant? http://www.sintmaartengov.org/Government%20Forms/Temp%20residency%20Permit%20Form%20-%20resguide1.pdf

St. Maarten and GDPR

- One of the main pillars of the St. Maarten economy is tourism. Caribbean hoteliers have been advised, by CHTA CEO Brian Kent, to become European Union (EU) General Data Protection Regulation (GDPR) compliant.
- Other organizations that should consider GDPR Compliance:
  - Airlines, Telecommunications, Harbor, Healthcare,
  - In general all organizations that actively provide services or goods to residents of St. Martin and St. Barth
  - All organizations that have a branch on one of the French islands
- Local organizations that have a direct business relationship EU based organizations could lose contract as a result of not being GDPR compliant
- Individuals or groups of people can start court case if there personal data was used other then in accordance to GDPR guidelines

St. Maarten and GDPR
Final comments

- The underlying intention of GDPR is to ensure that the terms of a business relationship are clear, consensual, and enforceable.
- The fundamental conflict is that neither the corporate world nor a legal framework will ultimately protect our privacy from being ravaged. **We have to take responsibility for your own Personal Data**: there is no other long-term option.
- We own our Personal Data — both physical and virtual — so we must take control.
  - we must act more like a landlord, and less like a powerless tenant

Thank you
Giovanni King

giovanniknng@gmail.com

+59995145464

BLUE SKY HOLDING