Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

May 2, 2018

ISOAG May 2, 2018

I. Welcome & Opening Remarks	Mike Watson, VITA
II. General Data Protection Regulation	Shana Bumpas, U of R
III. ISO Service Updates	Wes Kleene, VITA
IV. Upcoming Events	Mike Watson, VITA
V. Operations Update	NG

General Data Protection Regulation

Shana Bumpas, MSIA, CISSP, CRISC, CISA

Overview

- Approved into European Union (EU) law on April 14, 2016
  - Repeal’s EU Directive 95/46/EC
  - Consistency with privacy laws across EU
  - Protect and empower EU citizens’ data privacy
- Goes into effect **May 25, 2018** (23 days left)
- Penalties
  - The greater of 4% of annual global revenue or €20M ($24.17M)
  - Lower tier infraction is 2%
- Applies to EU Data Subjects
  - EU residents
  - US residents while physically in EU

Data Subject Rights

A data subject is a natural person

- the right to be informed;
- the right to be forgotten;
- the right of access;
- the right to rectification;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling

Legal Basis

The organization must have a lawful basis for processing personal data

There are six categories of lawful basis:

1. Consent
2. Contract
3. Legitimate interest
4. Legal obligation
5. Vital interest
6. Public authorities

Conduct legal basis impact assessment

Roles

- The controller is the entity that determines the purposes, conditions and means of the processing of personal data
- The processor is an entity which processes personal data on behalf of the controller
- Supervisory authority is EU regulator responsible for enforcement of the GDPR in relation to cross border processing
- Data Protection Officer (DPO) monitors compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

Types of Data

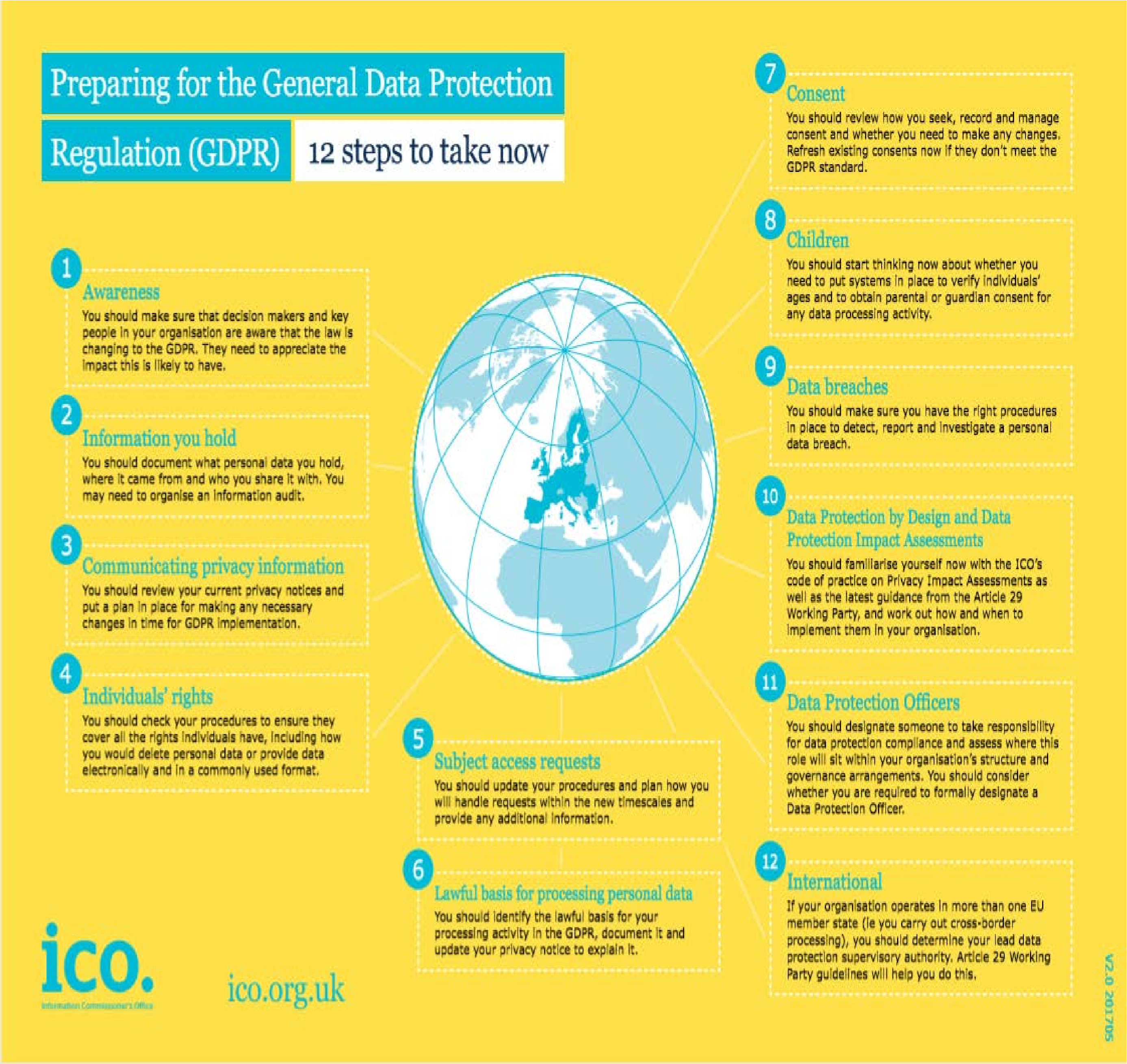
- “Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (European Parliament and the Council of the European Union, 2016).
- “Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation” European Parliament and the Council of the European Union, 2016).

Impact on Data Collection

- Data privacy impact assessment
  - Know where the data is
  - How it’s being used
- Consent
  - At collection
  - Clear about what is collected and how used
  - Ability to withdraw consent
  - Minors must have parents provide consent
  - Opt-in must be explicit
  - Lawful basis
- Privacy policy

Data Protections

- Privacy by design
- Pseudonymization
- Encryption – keys stored separately
- Breach notification within 72 hours or undue delay
- Privacy Shield (replaces Safe Harbor)
- DPO may be required
- EU Member States may have additional laws and compliance requirements



Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

V2.0 201705

Information Commissioner's Office, 2017

Next Steps…

- EU footprint
- Data privacy impact assessment
  - Data map
    - Identify data type and storage locations
    - Where it originates?
    - Permissions to collect
    - Why is it collected?
  - Evaluate current data processing practices
    - Review who has access
    - Record retention
  - Current compliance requirements

Questions

References

European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Information Commissioner's Office. (2017). "Preparing for the general data protection regulation (gdpr): 12 steps to take now." Retrieved from https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

Department of Commerce. (2018). Privacy Shield. Retrieved from https://www.privacyshield.gov/welcome.

Gydeline Ltd (2018, March 19). GDPR compliance journey 03 – data mapping. Retrieved from https://www.youtube.com/watch?v=W5D2gkbzQNk.

Information Security Program

Centralized ISO Security Services

J. Wesley Kleene, PhD, PE, CISM

Director, Centralized ISO Services

Charter

- Providing Information Security and Risk Management supporting to agencies, universities, commissions, boards, in the development, implementation, and effective operation of their information security program.

TEAM

Centralized ISO Security Services

- 31 (Agencies / Universities Commissions / Boards)
- 40% of the entities governed by CSRM
- Secretariats:
  - Administration
  - Agriculture and Forestry
  - Commerce and Trade
  - Education
  - Executive
  - Finance
  - Independent
  - Natural Resources
  - Public Safety
  - Transportation

Scope

Focus on:

- Risk Management and Information Security Program
- Business Impact Analysis (Business Process)
- System Security Plans / Risk Assessments
- Corrective / Risk Treatment Plans
- Risk reporting and tracking

Impacts and Updates

Business Processes

- Target BIA and Business Process reporting in eGRCS
- Connect business processes with functional needs
- Define the process with intent based on the agency mission
- Reduced from:
  - 30% of reported totals to 22% of reported totals
  - 14% of the Mission Essential Functions
  - Still a work in progress

Impacts and Updates

IT Systems / Applications

- Inventory development and reporting in eGRCS
- Link Systems with eGRCS elements providing common risk view
- Agencies account for approx. 28% of Systems

Interaction

What challenges do you see in your current environment need support?

Interaction

Do you see any security/risk management areas where a centralized service approach could provide benefit?

Contact Information

Wes Kleene, PhD, PE, CISM

Director, Centralized ISO Security Services

Wes.Kleene@vita.virginia.gov

804-416-6113

Upcoming Events

Future ISOAG

June 6, 2018 @ CESC 1:00-4:00

Speakers: Sherida Davis-Bryan,DOC

Alex Roeglin, APA

Michael Fitch & Prentice Kinser,SAIC

ISOAG meets the 1st Wednesday of each month in 2018

IS Orientation

When: **Thursday , June 7, 2018**

Time: **9:00 –11:00 am**

Where: **CESC , Room 1221**

Presenter: **Ed Miller**

Register here:

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

ISOAG meets the 1st Wednesday of each month in 2018

2018 IT Security Conference

The IS Conference Committee would like to extend a sincere thank you to those who attended the conference.

Please complete the Conference Survey to let us know how we can improve for 2019.

Survey link: https://www.surveymonkey.com/r/2018COVSECCONF

CPE information will be sent out next week

SAVE THE DATE

“2018 COVA Information Security Conference: “Expanding Security Knowledge"

April 11 & 12

Location: Altria Theater

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk