Measures for securing personal data flows

Yannick Scheelen - EY

The better the question. The better the answer.
The better the world works.

Belgium-Japan Association
Chamber of Commerce
日白協会兼商工会議所

Building a better working world

Agenda

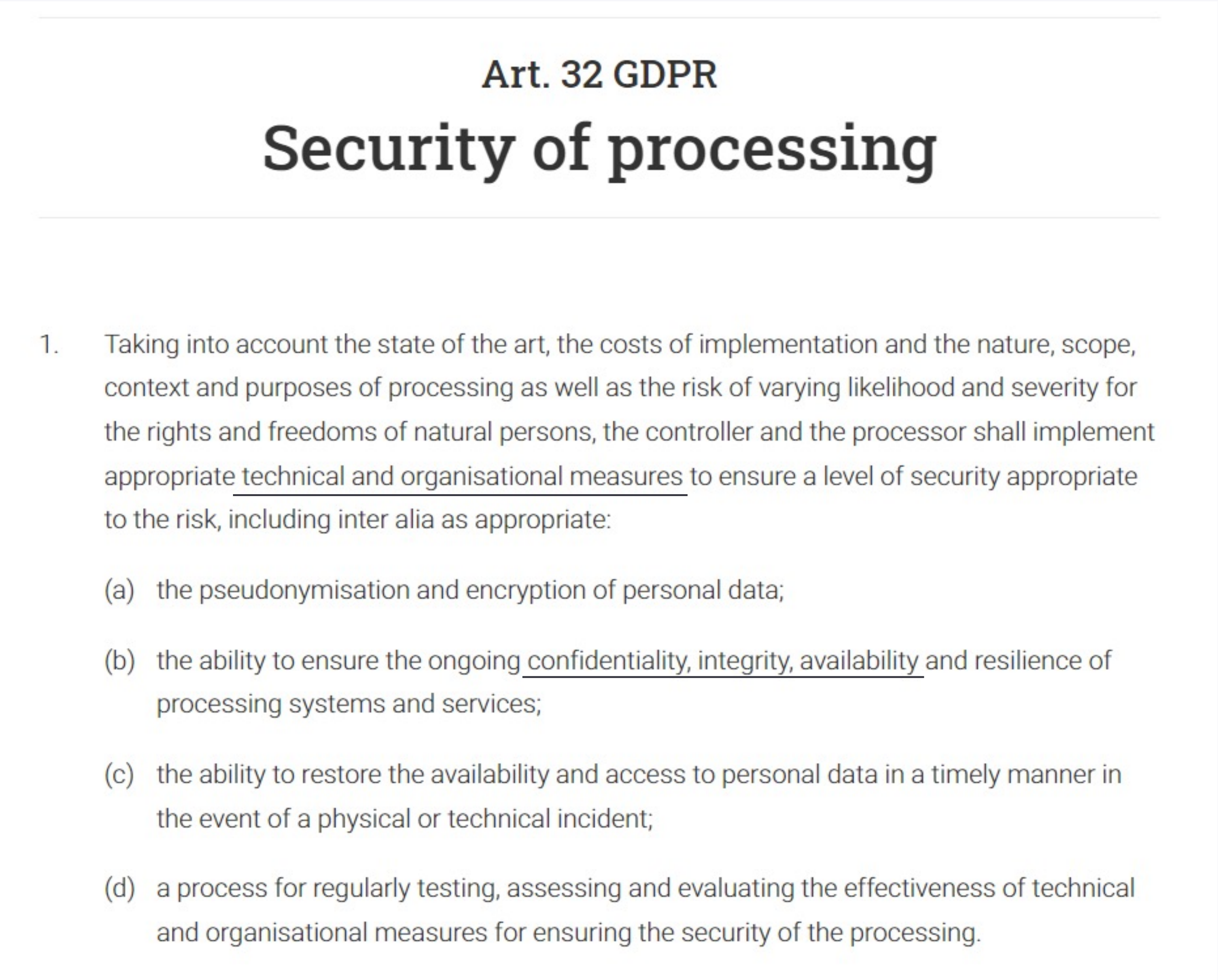
1. **Legality and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Restrictions on retention**
5. **Integrity, confidentiality & accountability**

Yannick Scheelen

SENIOR MANAGER- Cybersecurity & privacy

- Joined EY in 2012
- Focusses on a variety of cybersecurity and data privacy projects, for national and international clients across all sectors
- Experience with GDPR implementations and assessments since 2017

A short introduction – why cybersecurity for GDPR?



Art. 32 GDPR

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   (a) the pseudonymisation and encryption of personal data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

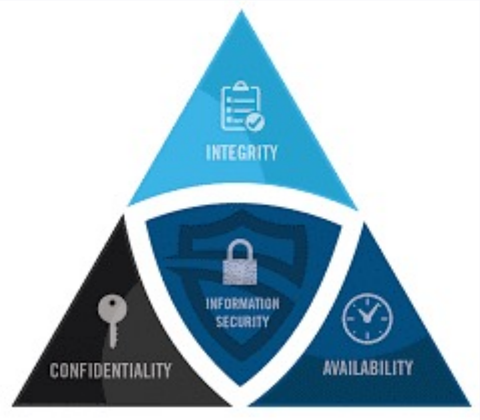
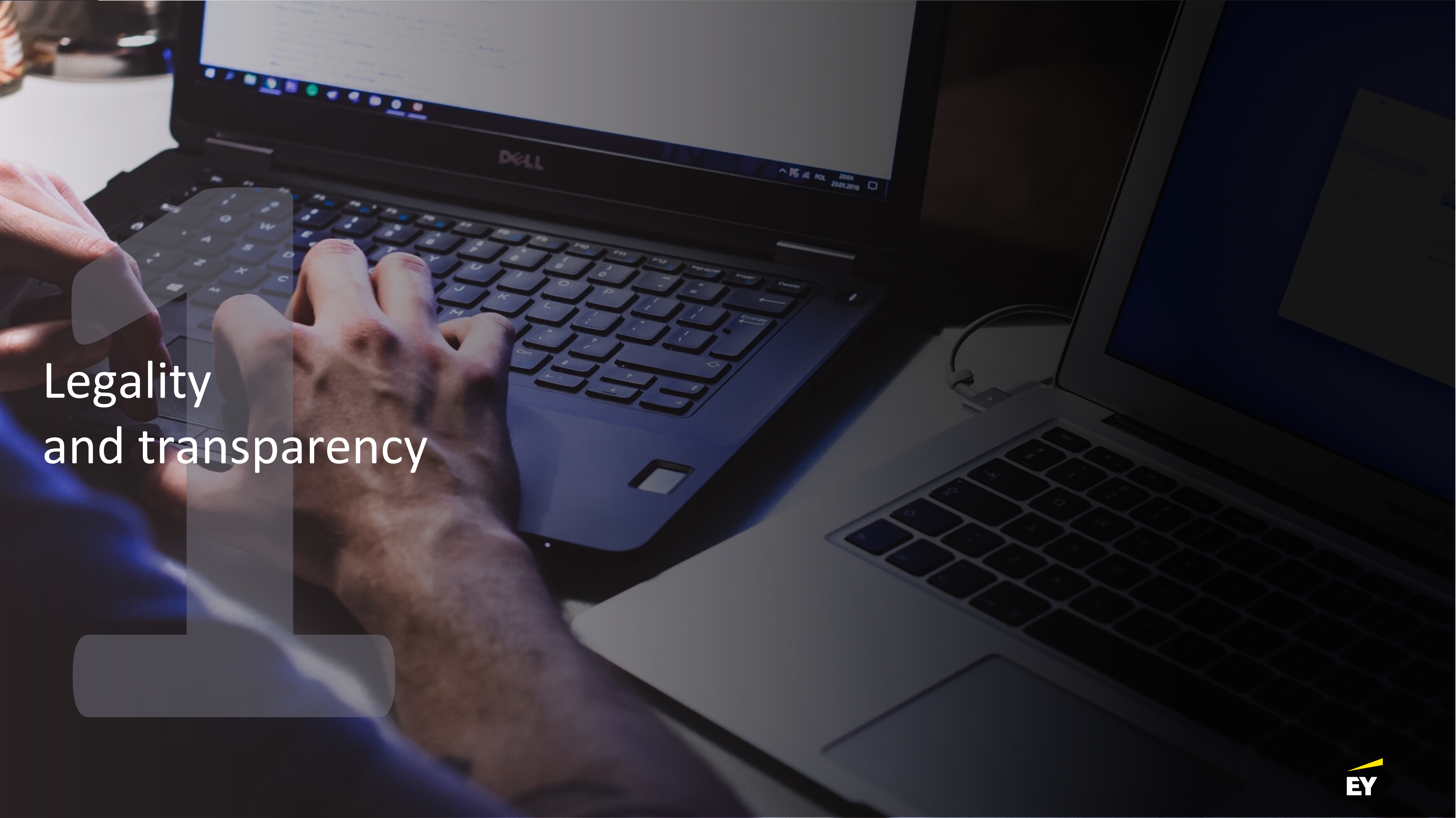


Figure: The cybersecurity CIA triad



1

Legality and transparency

EY
Building a better working world

01
02
03
04
05

Legality and transparency – Consent management

Legality and transparency

Consent management

> “ **Article 7(1) GDPR** - Where processing is based on consent, the controller must be able to demonstrate that the data subject has given consent to the processing of their personal data.

Data subjects must be informed of the processing at the time of collection of their personal data.

The consent must always be related to one specific purpose.
Linking the consent with different purposes is not allowed.

Data subjects must be able to withdraw their consent without any obligation, and this must happen as quickly and easily as giving consent.

The consent of the data subjects must be unambiguous. Standard ticked registration boxes are therefore forbidden.

✓ **Consent Management Platforms** (CMP) offer a central solution for documenting and managing the (online) consent of data subjects.

- Microsoft Dynamics Sales, Customer Service, ...
- OneTrust, TrustArc, Cookiebot, QuantCast, ...

✓ Provide **separate subscription or confirmation buttons** per purpose to adequately ensure granularity and specificity of consent.

- “Continuing to browse” does not constitute valid consent
- Cookies must be changeable after the first visit
  can be changed according to their category or purpose
- It is in principle not sufficient to merely
  refer to the browser settings to alter cookies

Legality and transparency – Consent management

01

02

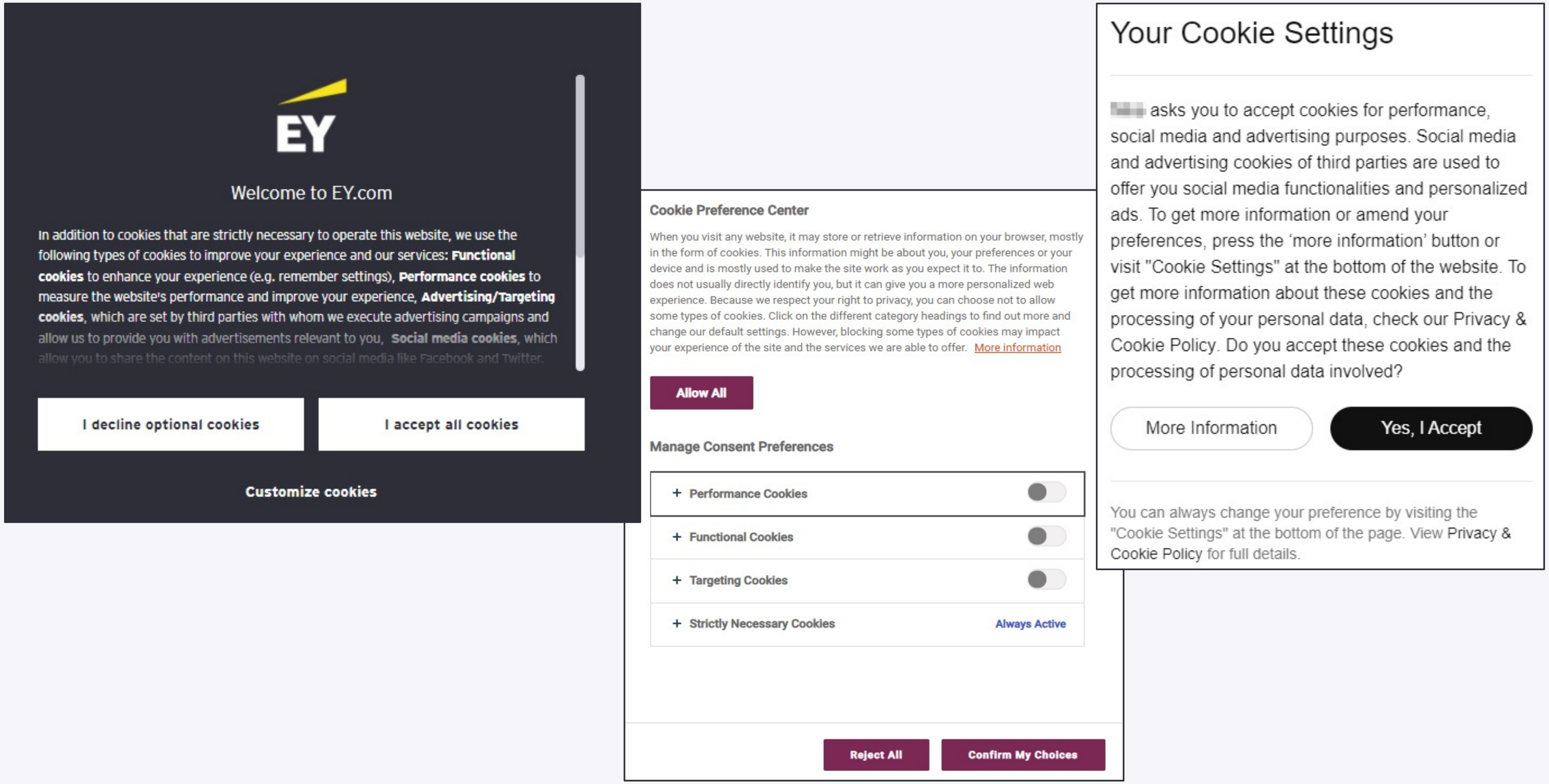
03

04

05

Legality and transparency

Consent management



Welcome to EY.com

In addition to cookies that are strictly necessary to operate this website, we use the following types of cookies to improve your experience and our services: **Functional cookies** to enhance your experience (e.g. remember settings), **Performance cookies** to measure the website's performance and improve your experience, **Advertising/Targeting cookies**, which are set by third parties with whom we execute advertising campaigns and allow us to provide you with advertisements relevant to you, **Social media cookies**, which allow you to share the content on this website on social media like Facebook and Twitter.

Cookie Preference Center

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer. More information

Manage Consent Preferences

- + Performance Cookies ○
- + Functional Cookies ○
- + Targeting Cookies ○
- + Strictly Necessary Cookies Always Active

Your Cookie Settings

[redacted] asks you to accept cookies for performance, social media and advertising purposes. Social media and advertising cookies of third parties are used to offer you social media functionalities and personalized ads. To get more information or amend your preferences, press the 'more information' button or visit "Cookie Settings" at the bottom of the website. To get more information about these cookies and the processing of your personal data, check our Privacy & Cookie Policy. Do you accept these cookies and the processing of personal data involved?

You can always change your preference by visiting the "Cookie Settings" at the bottom of the page. View Privacy & Cookie Policy for full details.

2

Purpose limitation

EY
Building a better working world

01

02

03

04

05

Purpose limitation – Further processing of personal data

Purpose limitation

Further processing of personal data

Encryption of personal data

> **Article 5(1)(b) of the GDPR** - Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes.

Inform all stakeholders (internal employees, processors...) about the purposes for which personal data may be processed.

Limit the possibilities of unauthorised processing or access of personal data by disabling unnecessary functionalities.

Monitor the use of ICT infrastructure, systems and networks to detect excessive or unwanted use of personal data.

If prior consent cannot be obtained for further processing, the new processing purpose must be compatible with the initial purposes.

✓ Establish an **internal policy** on the **use of personal data** within the organisation.

- Acceptable Use Policy, Code of Conduct

✓ Use built-in **analytics** functionalities to **monitor** the **use of ICT**, subject to applicable regulations.

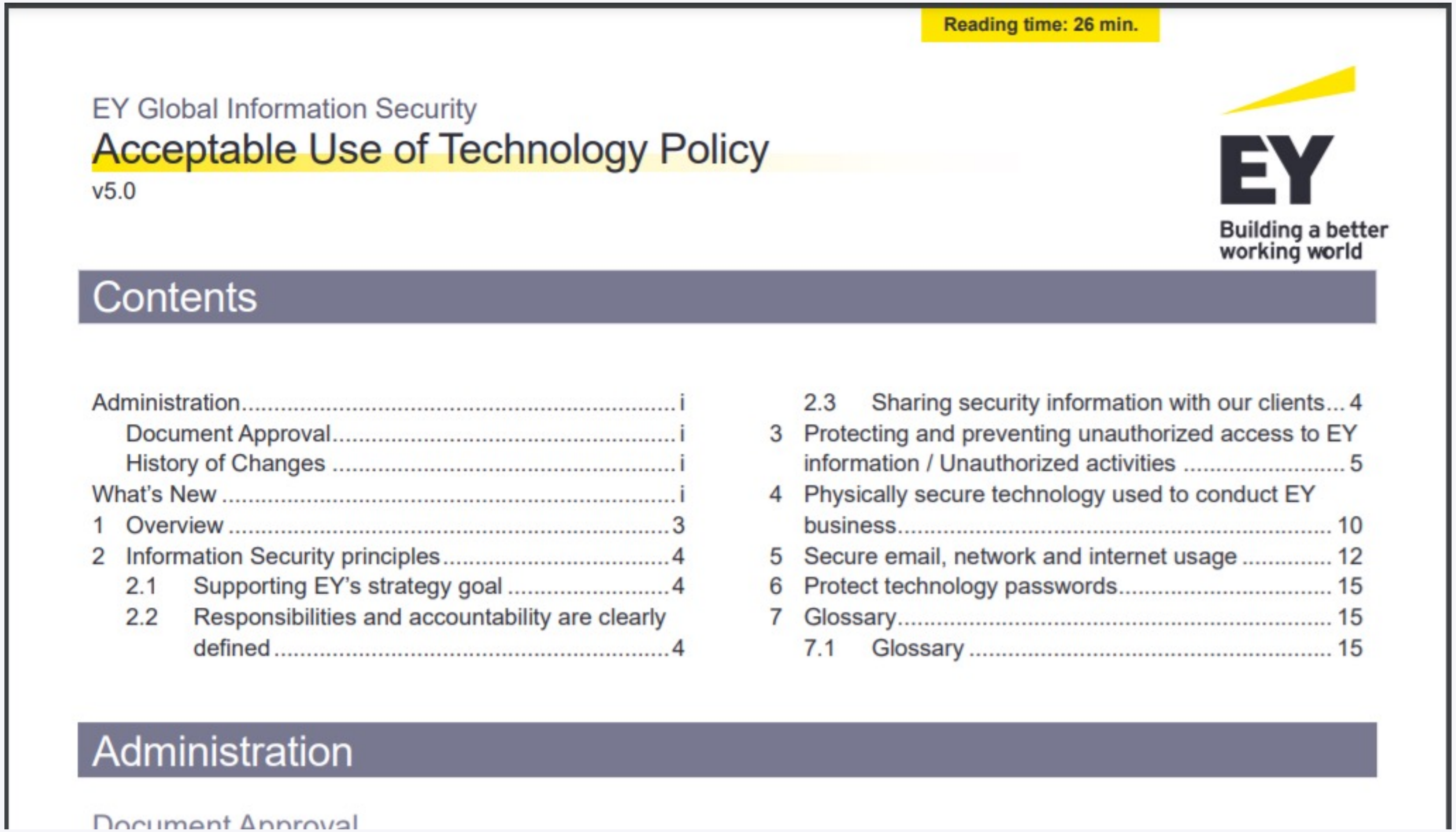
- Data Leakage Prevention

Purpose limitation – Further processing of personal data

Purpose limitation

Further processing of personal data

Encryption of personal data



Reading time: 26 min.

EY Global Information Security

Acceptable Use of Technology Policy

v5.0

Building a better working world

Contents

Administration

Document Approval

Purpose limitation – Further processing of personal data

01

02

03

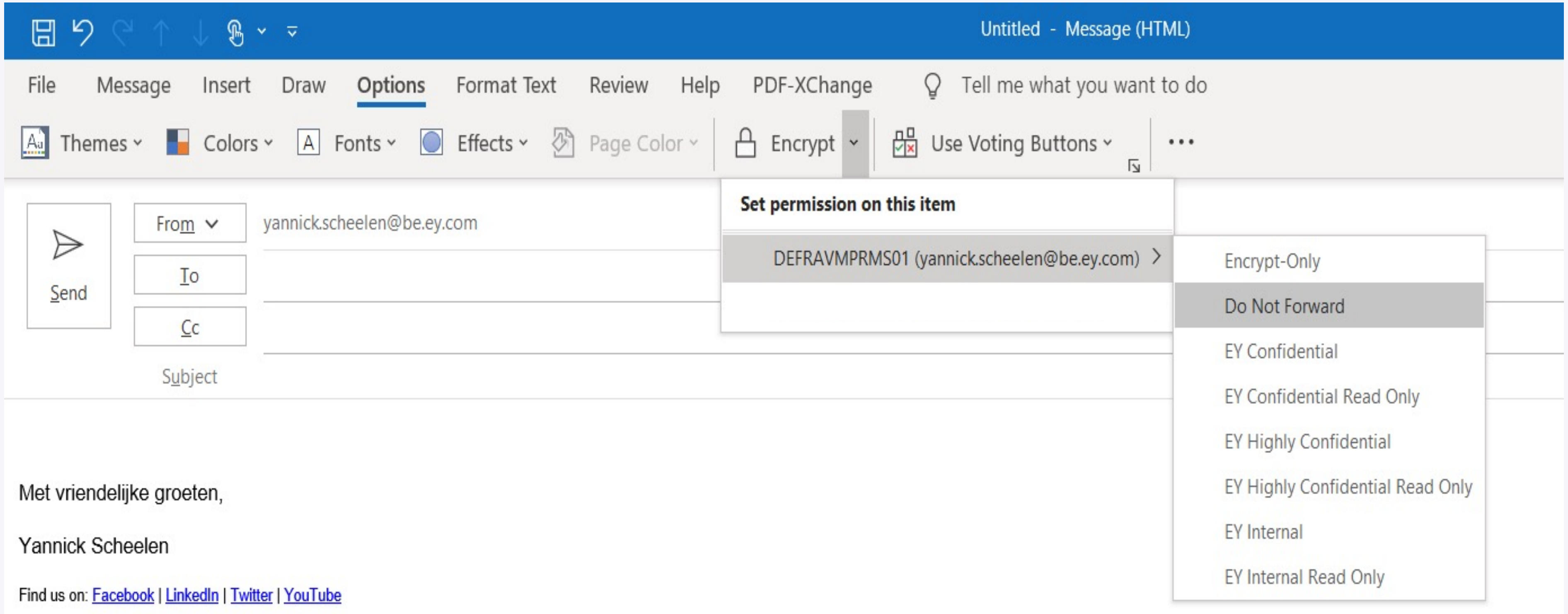
04

05

Purpose limitation

Further processing of personal data

Encryption of personal data



yannick.scheelen@be.ey.com

Set permission on this item

DEFRAVMPRMS01 (yannick.scheelen@be.ey.com)

- Encrypt-Only
- Do Not Forward
- EY Confidential
- EY Confidential Read Only
- EY Highly Confidential
- EY Highly Confidential Read Only
- EY Internal
- EY Internal Read Only

Met vriendelijke groeten,

Yannick Scheelen

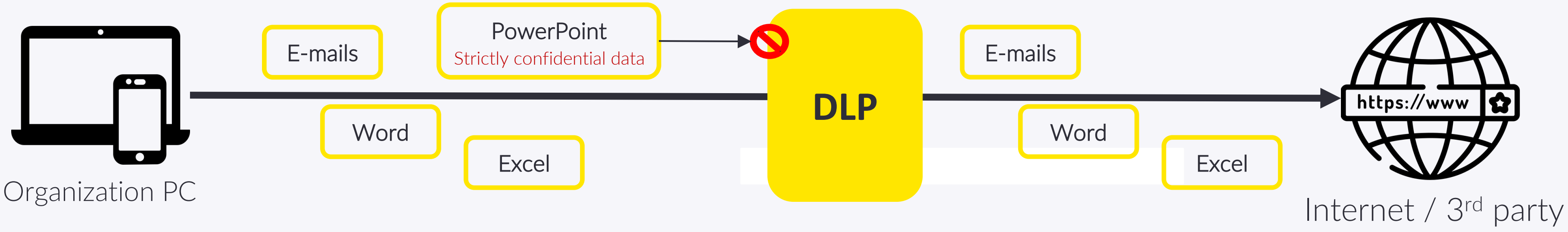
Find us on: Facebook | LinkedIn | Twitter | YouTube

Purpose limitation – Further processing of personal data

Purpose limitation

Further processing of personal data

Encryption of personal data



Purpose limitation – Encryption of personal data

Purpose limitation

Further processing of personal data

Encryption of personal data

> Data is stored and shared with others in various ways. It should also be brought to attention that the storage or exchange of this data needs to occur in a secure manner.

Applications and websites of controllers should use secure protocols (HTTPS/TLS) to ensure that data is sent in a secure and encrypted way.

Implementation of security measures for e-mails (STARTTLS, DKIM, SPF) to ensure that both the integrity and confidentiality are preserved.

Enable BitLocker on end-user devices and peripherals to ensure that these files are encrypted.

Encryption and security measures can be applied to on-premise servers or data in the cloud.

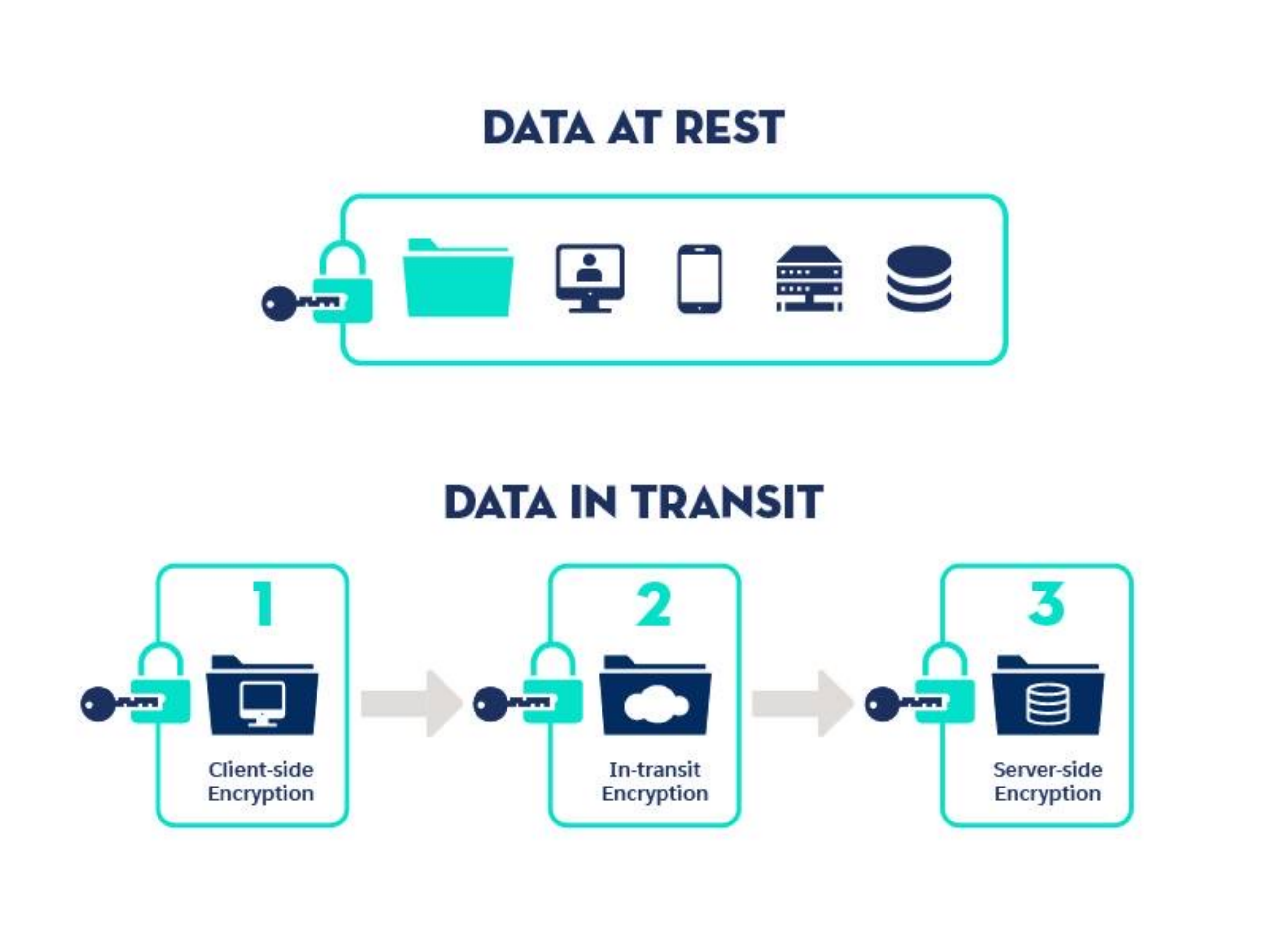
✓ When developing applications, make use of **secure coding standards** and the OWASP top 10 to ensure that safety of the data is guaranteed.

✓ Share files through **a single platform** such as SharePoint to ensure that the necessary protection measures can be applied and the data is not lost in other forms of communication such as e-mail.

✓ Make employees aware of the use of a safe of a **secure internet connection**. Encourage them to use the VPN when reliable networks are not available.

✓ Include end user devices in a **Mobile Device Management** application (fe. Intune) so that if the device is stolen or lost, the data can be erased.

Encryption of personal data – Encryption of data



01

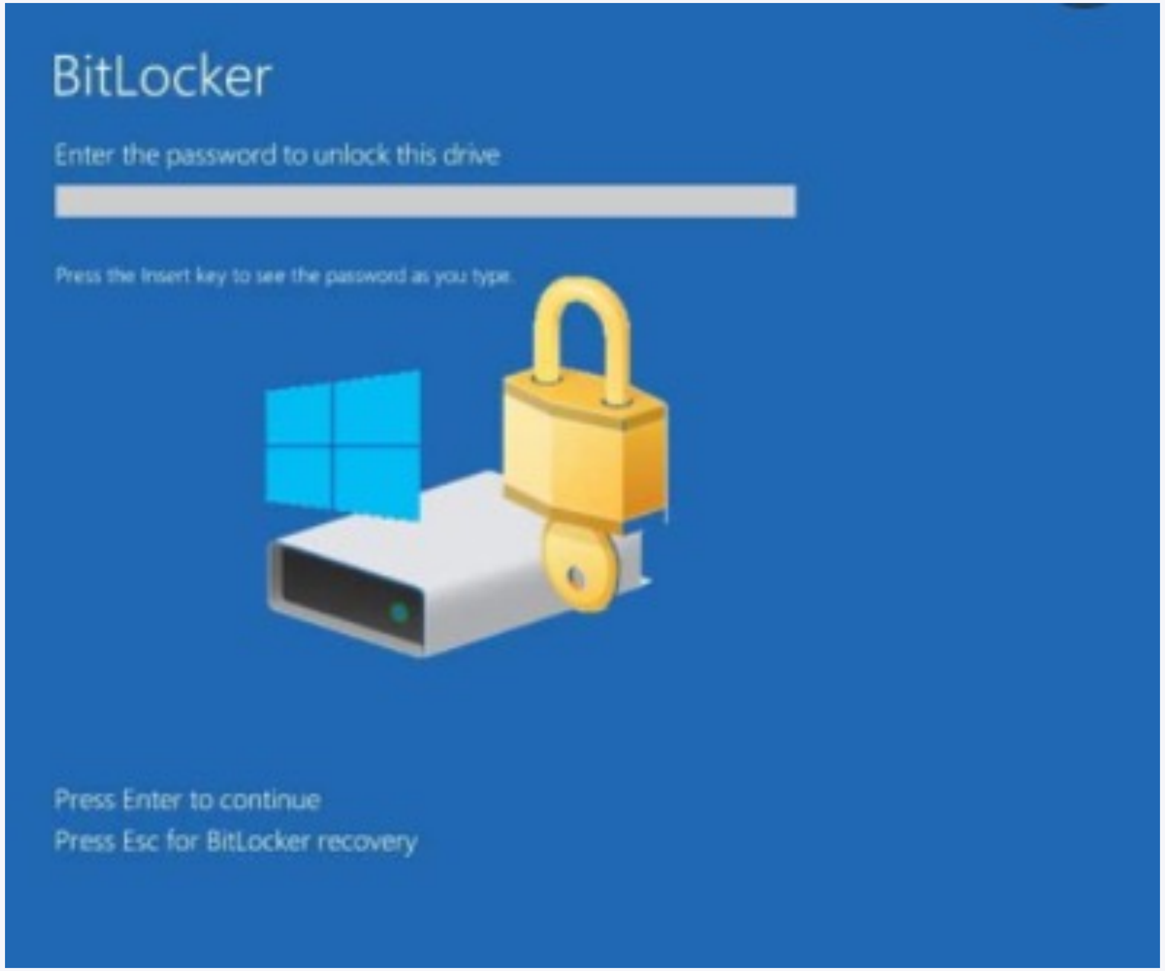
02

03

04

05

Encryption of personal data – Encryption of data at rest



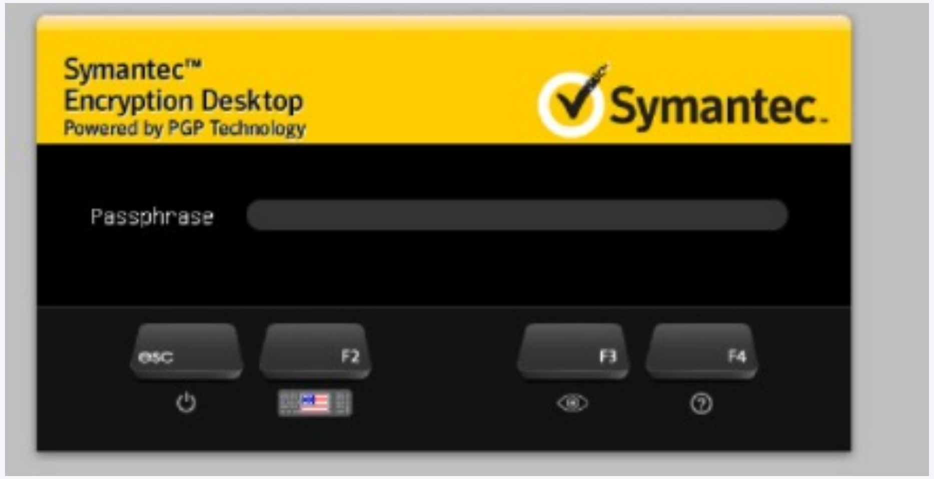
BitLocker

Enter the password to unlock this drive

Press the Insert key to see the password as you type.

Press Enter to continue

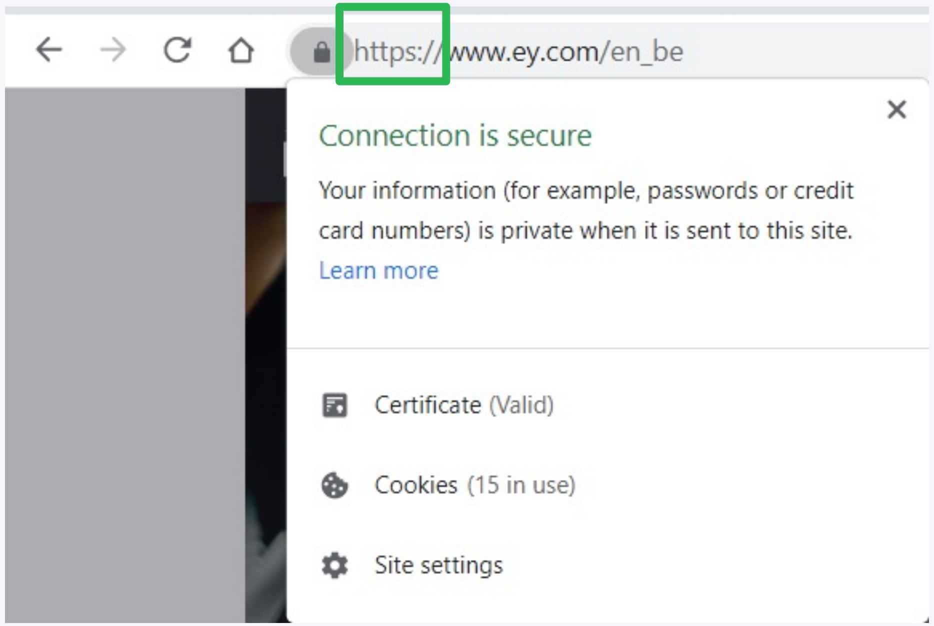
Press Esc for BitLocker recovery



Symantec™ Encryption Desktop
Powered by PGP Technology

Passphrase

Encryption of personal data – Encryption of Internet traffic



https://www.ey.com/en_be

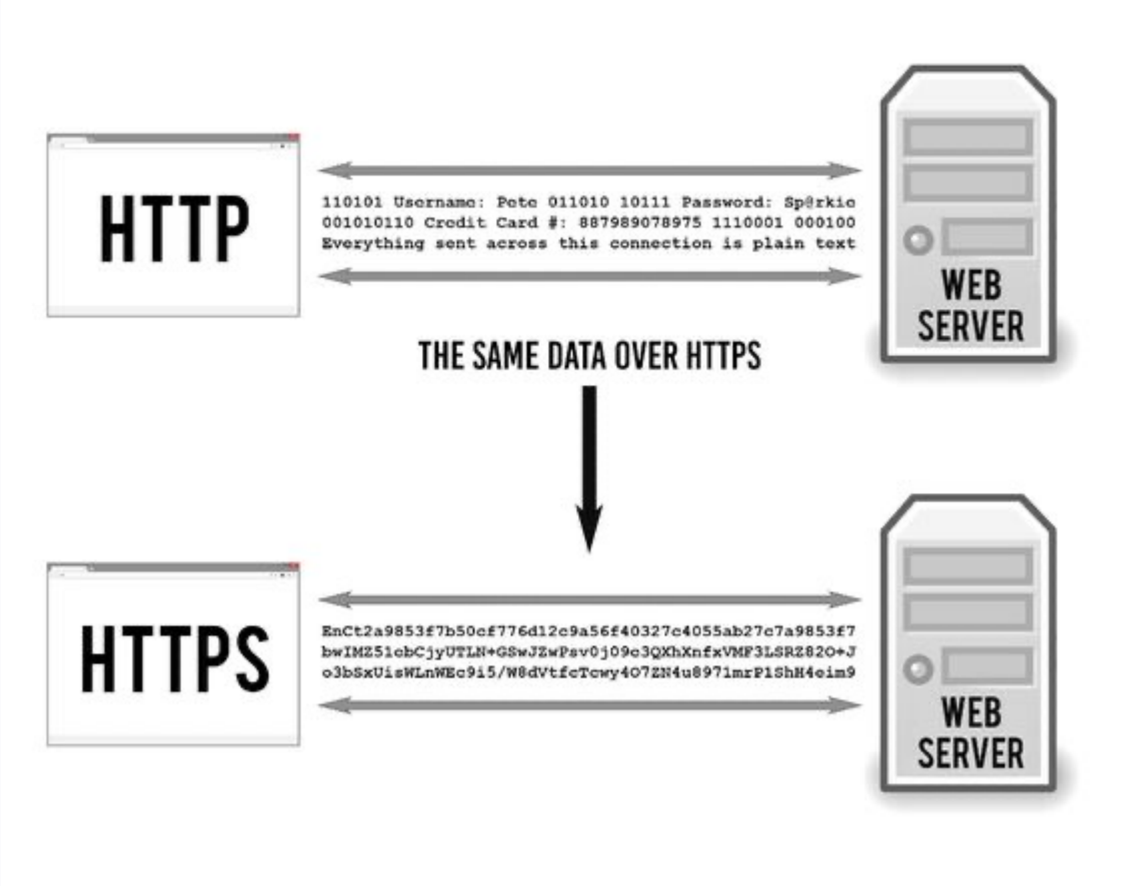
Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

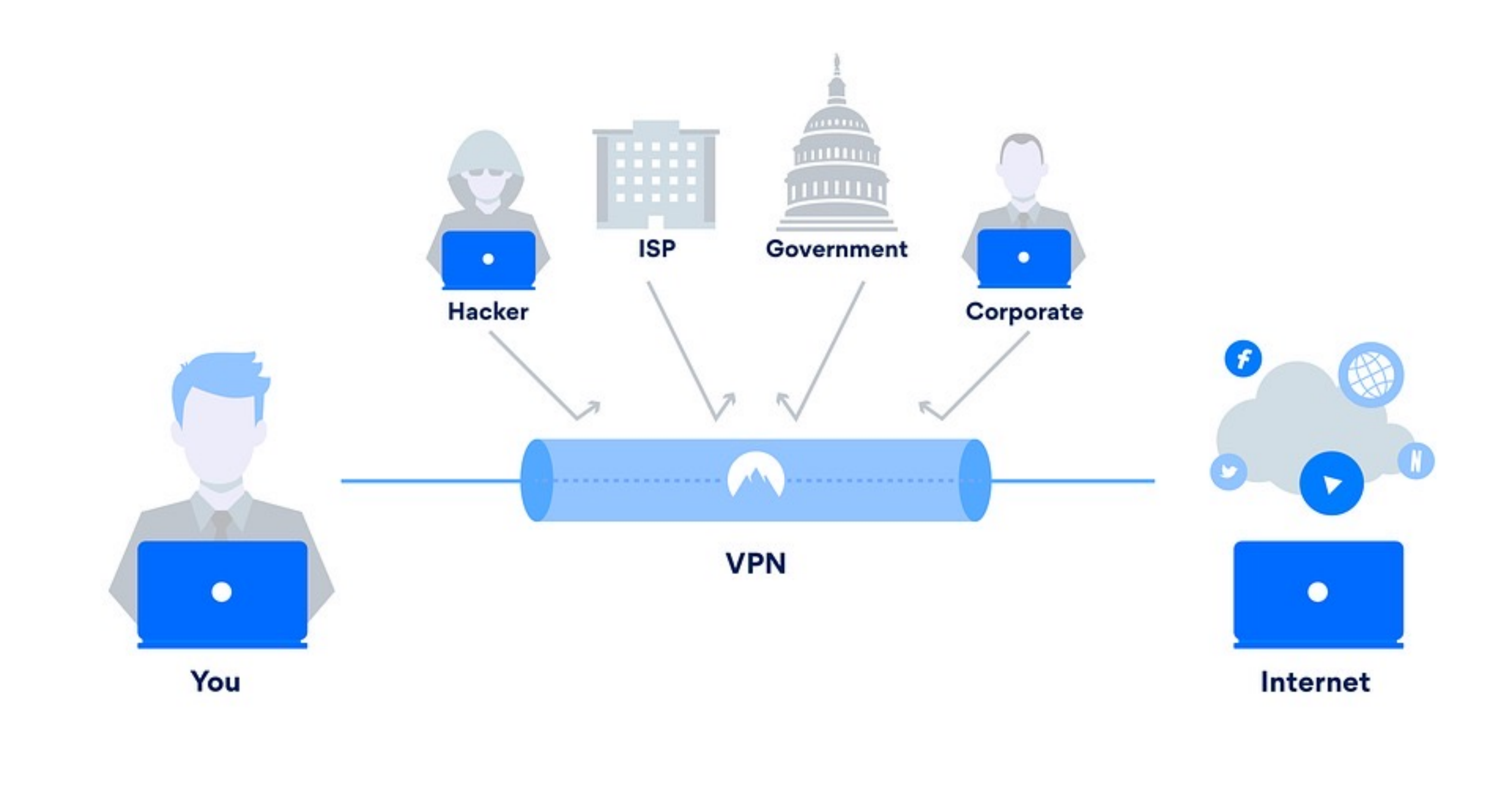
Certificate (Valid)

Cookies (15 in use)

Site settings

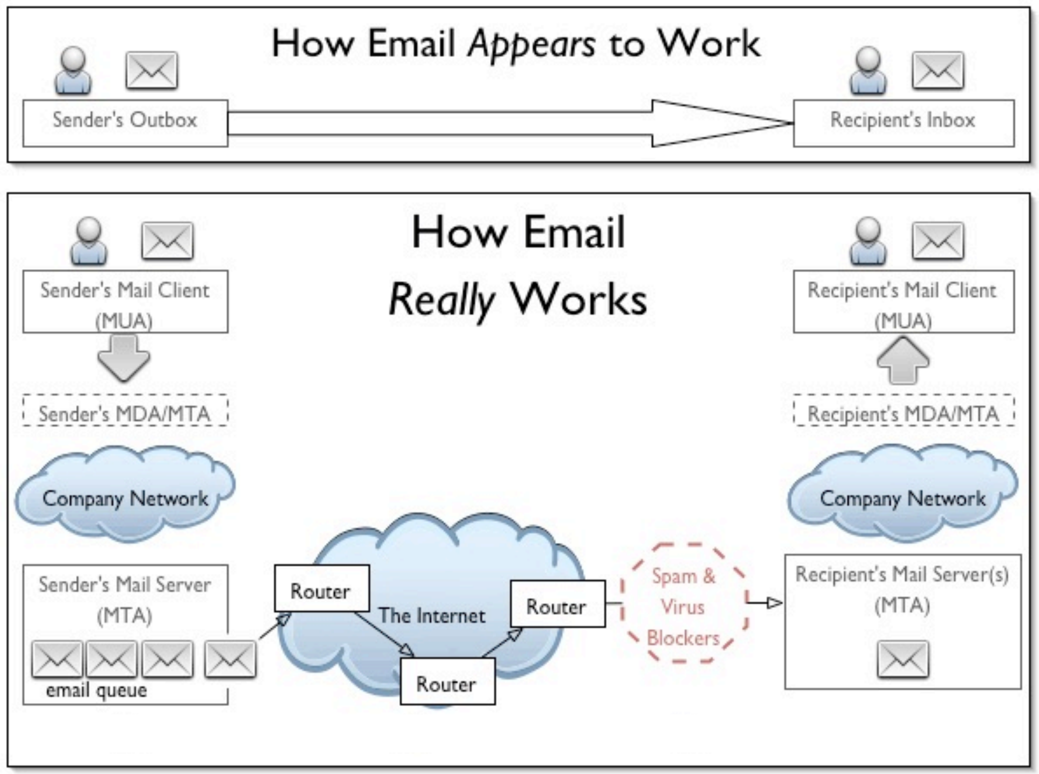

HTTP
110101 Username: Pete 011010 10111 Password: Sp@rkie
001010110 Credit Card #: 887989078975 1110001 000100
Everything sent across this connection is plain text
WEB SERVER
THE SAME DATA OVER HTTPS
HTTPS
EnCt2a9853f7b50cf776d12c9a56f40327c4055ab27c7a9853f7
bwIMZ51cbCjyUTLN+GSwJZwPsv0j09c3QXhXnfxVMF3LSRZ820+J
o3bSxUisWLnWEc9i5/W8dVtfcTcwy407ZN4u8971mrP1ShH4eim9
WEB SERVER

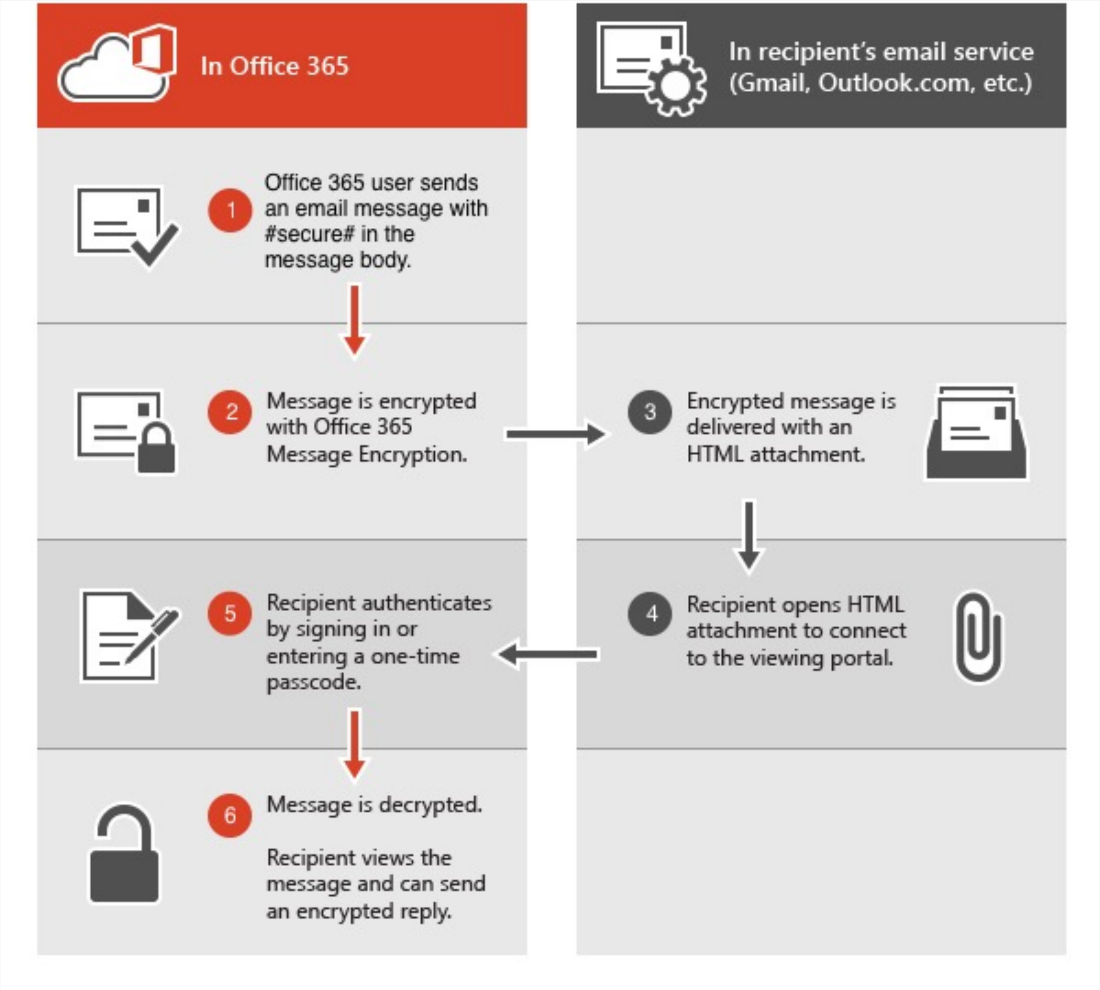
Encryption of personal data – Encryption of Internet traffic



01
02
03
04
05

Encryption of personal data – Encryption of e-mail





1 Office 365 user sends an email message with #secure# in the message body.

2 Message is encrypted with Office 365 Message Encryption.

3 Encrypted message is delivered with an HTML attachment.

4 Recipient opens HTML attachment to connect to the viewing portal.

5 Recipient authenticates by signing in or entering a one-time passcode.

6 Message is decrypted.

Recipient views the message and can send an encrypted reply.

Encryption of personal data – Encryption of e-mail

01

02

03

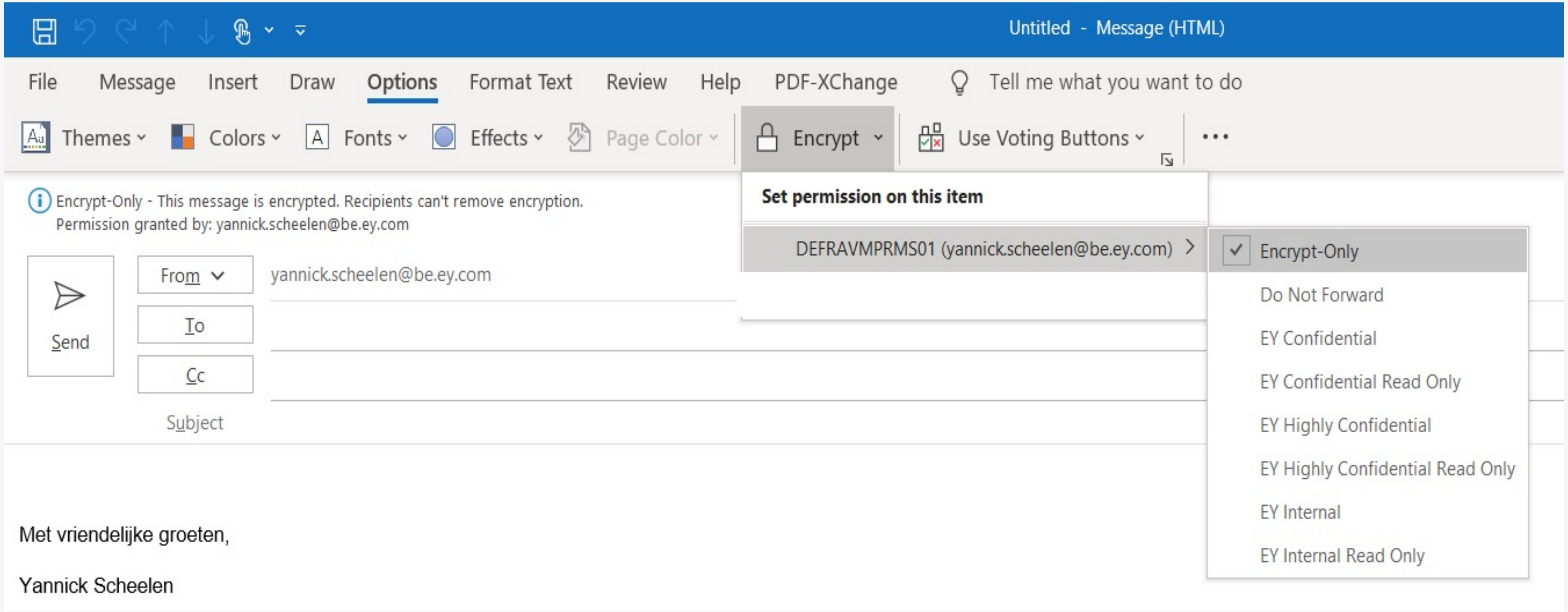
04

05

Purpose limitation

Further processing of personal data

Encryption of personal data



Encrypt-Only - This message is encrypted. Recipients can't remove encryption.
Permission granted by: yannick.scheelen@be.ey.com

From: yannick.scheelen@be.ey.com

Set permission on this item

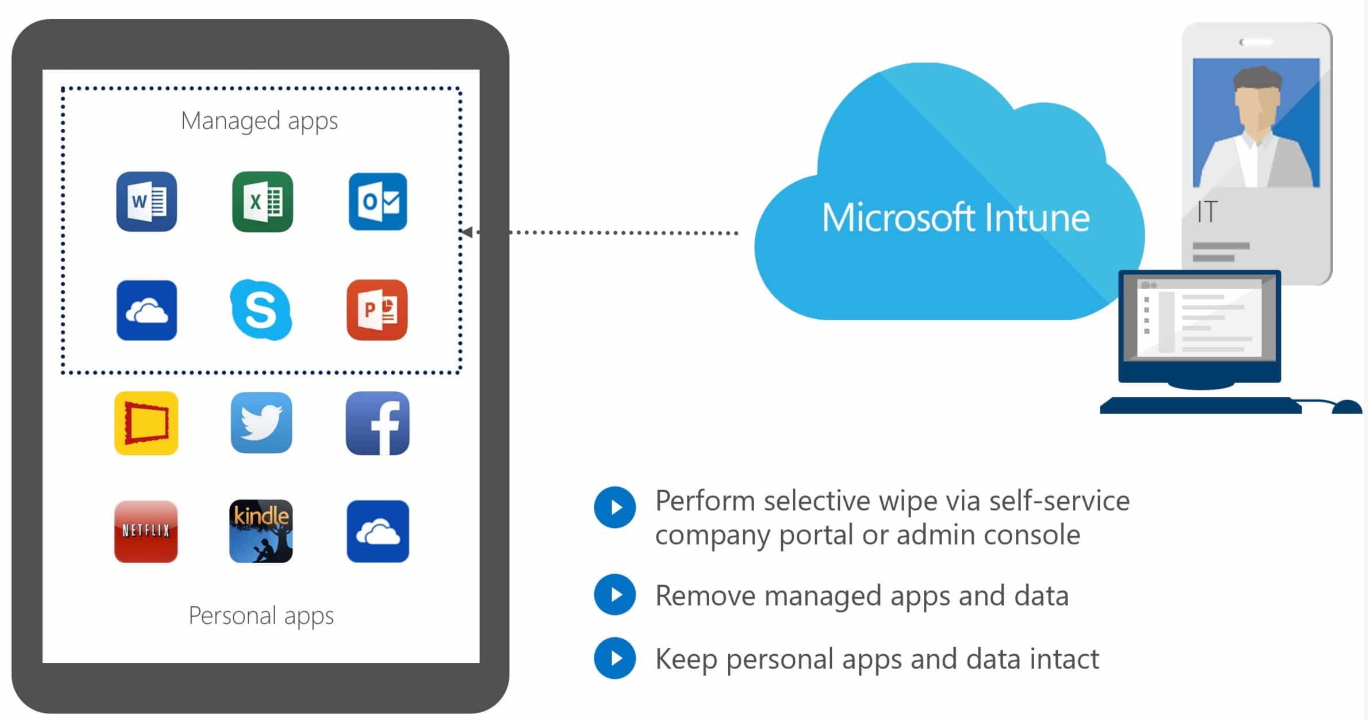
DEFRAVMPRMS01 (yannick.scheelen@be.ey.com)

- ✓ Encrypt-Only
- Do Not Forward
- EY Confidential
- EY Confidential Read Only
- EY Highly Confidential
- EY Highly Confidential Read Only
- EY Internal
- EY Internal Read Only

Met vriendelijke groeten,

Yannick Scheelen

Encryption of personal data – Mobile device management



- Perform selective wipe via self-service company portal or admin console
- Remove managed apps and data
- Keep personal apps and data intact

3

Data minimisation

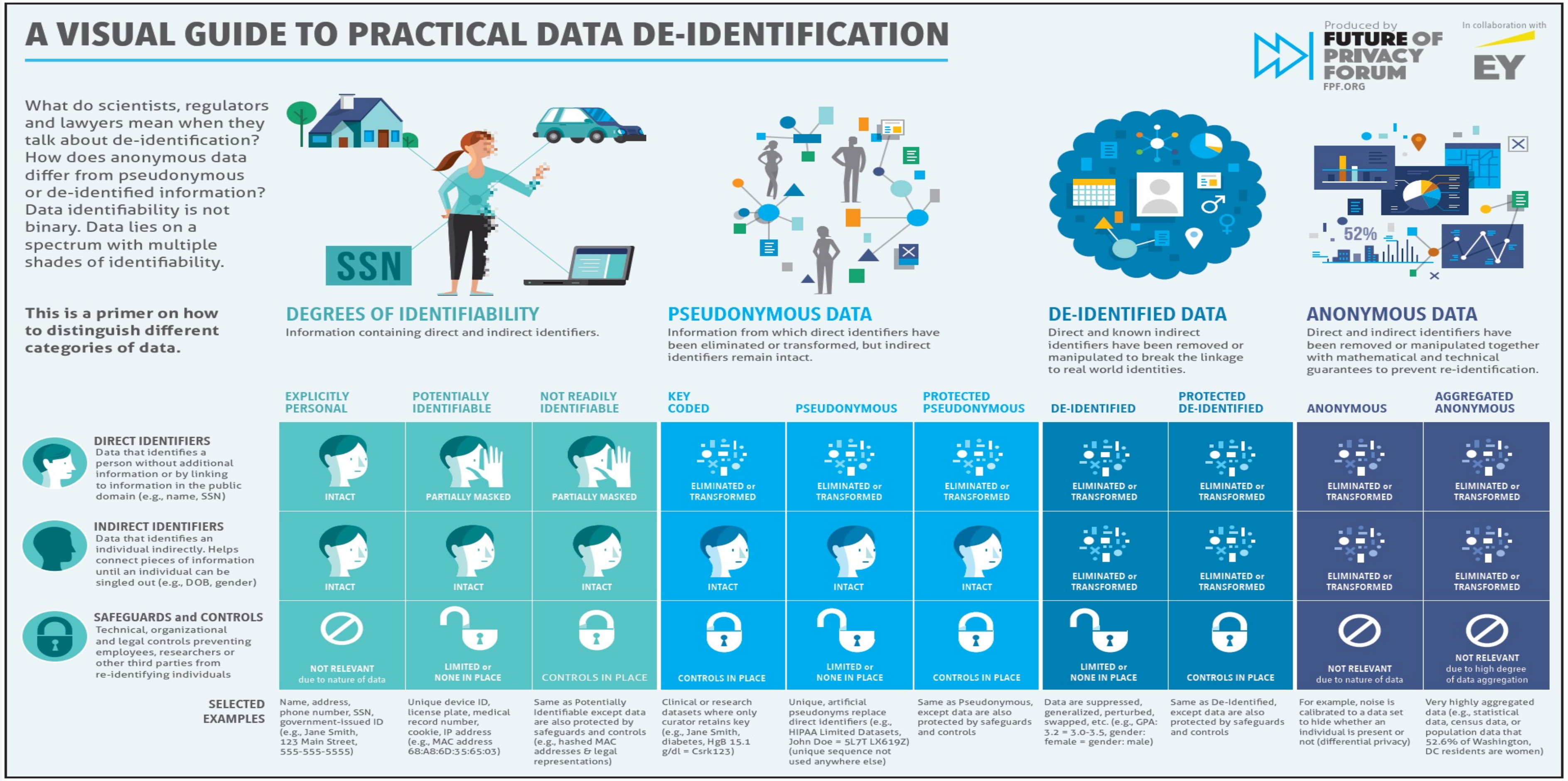
Data minimisation – pseudonymization vs. anonymization

01
02
03
04
05

Minimum data processing

De-identification

> **Article 5(1)(c) GDPR** - Personal data shall be adequate, relevant and limited to what is necessary for the purposes of the processing.



A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM FPF.ORG

In collaboration with EY

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.

This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

4 Storage restriction

EY
Building a better working world

01

02

03

04

05

Storage restriction – Retention periods

Storage restriction

Storage periods

> **Article 5 (1)(e) GDPR** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Define a retention period for each dataset in a policy, after consultation with stakeholders and in accordance with applicable regulations.

Sometimes several retention periods may apply to one file. In that case controllers will have to delete the personal data that are no longer necessary.

Sometimes several retention periods may apply to one file. In that case controllers will have to delete the personal data that are no longer necessary.

The main IT service providers offer functionalities in their software that allow controllers to record and automatically roll out retention periods within the organization.

✓ For each dataset, unambiguously determine when the retention periods start to run.

- At the time of initial collection
- From the last interaction with the data subject, ...

✓ With *retention policies* and *labels*, controllers can easily configure retention periods in Microsoft 365.

- *Retention policies* offer the possibility to set the same retention period on an entire site, OneDrive, Teams channel or mailbox
- *Retention labels* allow to define separate retention periods for each item (e.g. a folder, a file or an e-mail)
- Retention periods can start on the creation date or last change of the data
- In contrast to *policies*, the configured retention periods using *labels* continue to apply regardless of whether a file is moved to another repository or not.
- *Retention labels* can be configured manually or automatically (by keywords, attributes or the nature of the data)

01

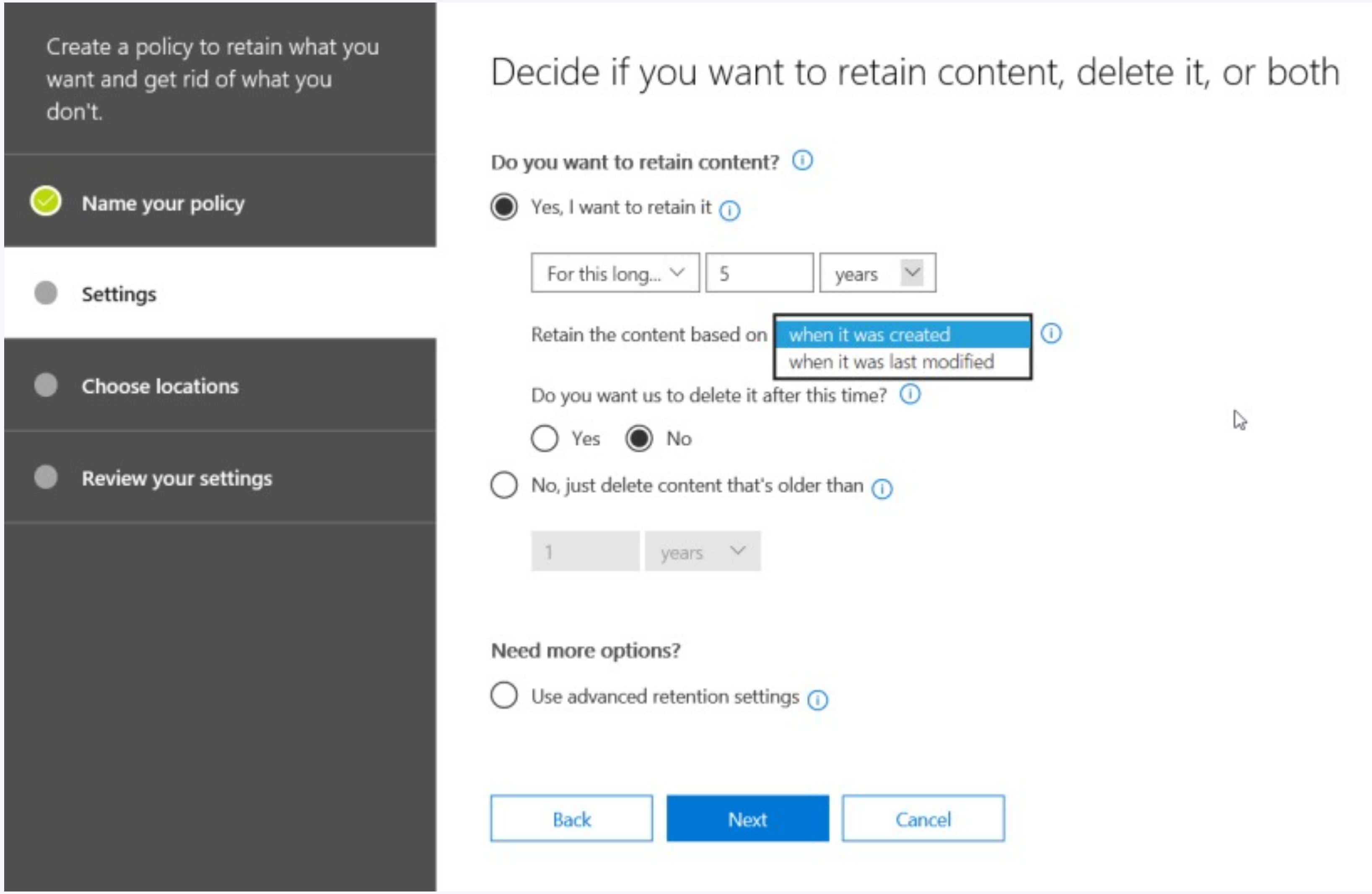
02

03

04

05

Storage restriction – Retention periods



Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ● Settings
- ● Choose locations
- ● Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

● Yes, I want to retain it ⓘ

For this long... | 5 | years

Retain the content based on: when it was created ⓘ
- when it was created
- when it was last modified

Do you want us to delete it after this time? ⓘ

○ Yes ● No

○ No, just delete content that's older than ⓘ

1 | years

Need more options?

○ Use advanced retention settings ⓘ

5

Integrity, confidentiality and accountability

Data access – Identity and Access Management (IAM)

> IAM enables the organization to grant users, employees or contractors with the correct accesses and to review the corresponding access rights based on their roles.

IAM is a collective name for products, processes and policies used to manage identities and access rights.

IAM systems are designed to perform three important tasks: identify, authenticate and authorise.

An IAM policy enables controllers to identify violations more easily, remove inappropriate access rights and revoke access when necessary.

Limits internal threats, as employees can only access the systems they need to perform their specific tasks.

✓ Granting employees access to data is a difficult process. Use a strong model to ensure that access is managed coherently.

✓ Accesses should be given based on a user’s role, or other attributes that are relevant to the employee.

Data access – Best practices

Integrity, confidentiality and accountability

Access to data

Data classification

Technical standards

Training and awareness

- Enforcing a strong password policy
- Audit existing accesses and rights on a regular basis
- Handle carefully when granting new accesses and rights
- Least-Privilege Model, Zero Trust
- Multi-Factor Authentication (MFA)
- Do not use privileged accounts for daily operations

Data classification – Introduction

> Classifying information helps the organization to improve their data structure and ensure the confidentiality of the content.

Employees are more aware of the type of information they are dealing with and their obligations to protect it to prevent data loss.

By classifying data, assigning labels and enforcing policies, controllers can comply with legal and regulatory requirements.

By classifying data, controllers can prepare to identify the risk and impact of an incident based on the type of data involved.

By understanding the sensitivity of the data, controllers can identify who should or should not have access to it, both inside and outside your organization.

✓ Establish a classification policy that uses criteria that are simple and avoid ambiguity, but are generic enough to apply to different datasets and circumstances.

✓ For an ideal operation, a classification scheme should be created using at least 3 and no more than 5 levels. The higher the level, the higher the authority.

✓ The classification of information applies to emails, documents and folders as well as to a wider IT environment such as Microsoft O365 (Teams, OneDrive, SharePoint and Exchange).

✓ The created classification labels can be further used in Data Loss Prevention (DLP) and Data Retention within Microsoft O365 (E5) or another external application.

Data classification – Principles and schemes

01
02
03
04
05

Integrity, confidentiality and accountability

Access to data

Data classification

Technical standards

Training and awareness

- Classification of information is based on three standard principles:

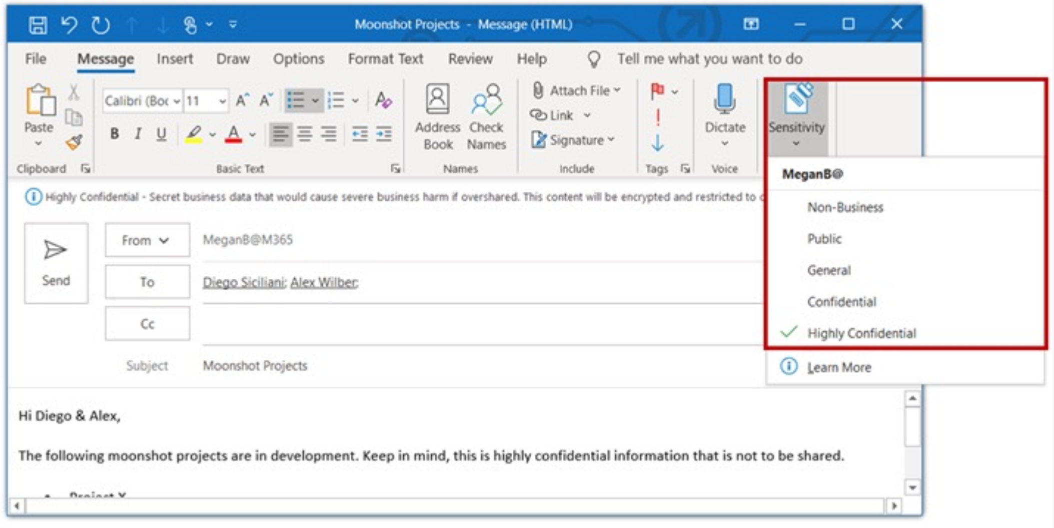
Availability	Integrity	Confidentiality
Information should be consistent and easily accessible by authorized parties.	Includes maintaining the consistency, accuracy and reliability of information throughout its lifecycle.	Preventing unauthorized access from sensitive information.

- Example of classification scheme:

Public	Internal Use	Confidential	Highly Confidential
Data that does not require special protection and may be freely disclosed.	Internal data not intended for public disclosure. If the data is compromised, it would have a minimal impact, but would not affect controller's profitability or operations.	Highly sensitive company and customer data which, if disclosed, could put controllers at risk, lose a customer or disrupt business operations.	Data considered most critical to controllers. Disclosure of this data may violate or have serious implications for regulations.

01
02
03
04
05

Data classification – Assigning labels



Highly Confidential - Secret business data that would cause severe business harm if overshared. This content will be encrypted and restricted to

MeganB@

- Non-Business
- Public
- General
- Confidential
- ✓ Highly Confidential

From: MeganB@M365

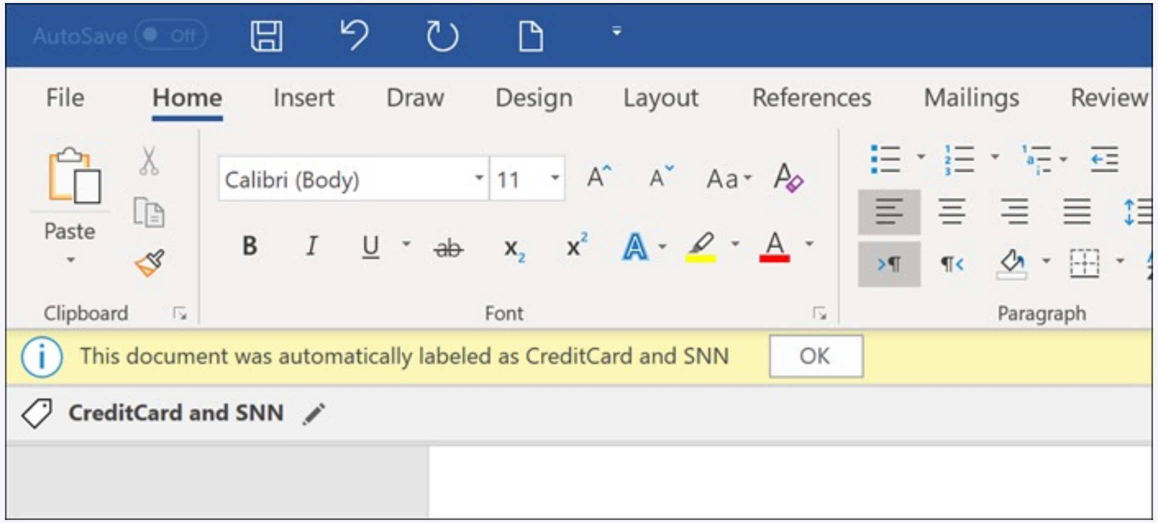
To: Diego Siciliani; Alex Wilber;

Subject: Moonshot Projects

Hi Diego & Alex,

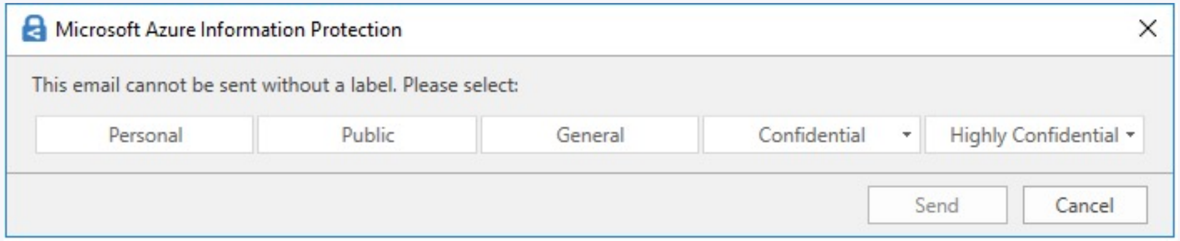
The following moonshot projects are in development. Keep in mind, this is highly confidential information that is not to be shared.

- Project X



This document was automatically labeled as CreditCard and SNN

CreditCard and SNN


Microsoft Azure Information Protection

This email cannot be sent without a label. Please select:

Accountability – Standards and audits

> **Article 5 (2) of the GDPR** - The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

ISO 27001 is a recognized roadmap for the development, implementation and management of an integrated information security programme, but it is not an GDPR certification.

Organizations are increasingly exposed to targeted cyber attacks on their IT systems and applications, which exploit known vulnerabilities.

Perform regular (internal) audits of the IT infrastructure to expose and timely remedy vulnerabilities in the security systems.

Before using a processor, controllers shall check whether the processor offers adequate guarantees with regard to the protection of personal data.

✓ By means of an **ISO 27001 (ISMS)** certification, controllers can demonstrate that **management measures** have been taken regarding **information security**.

✓ With the additional **ISO 27701 (PIMS)** certification, controllers can also demonstrate that the organization has taken appropriate security measures and safeguards with respect to **personal data**.

✓ The **ISO 27018** standard is specifically intended for providers of **cloud services**. With this certification, they can demonstrate adequate maturity regarding the protection of personal data in the cloud.

✓ Third Party Risk Management

✓ The 20 **CIS controls** form a set of prioritized actions with which organizations can protect themselves against the most known or the most common cyber attacks.

01

02

03

04

05

Accountability – Training and awareness

Integrity, confidentiality and accountability

Access to data

Data classification

Technical standards

Training and awareness

> “ **Article 39 (1)(b) GDPR** - The Data Protection Officer shall perform at least the following tasks:
> monitoring compliance with the GDPR, including awareness-raising and training of the staff involved in the processing.

Workshops increase interactivity with the participants and allow for content tailored.

eLearnings offer the possibility to better monitor the participation and knowledge of employees on an individual level.

Regular internal communications promote continuous awareness of privacy throughout the organization.

A privacy-conscious organization can rely on its employees to report some privacy issues in time to the right persons (DPO) or deal with them independently.

✓ When recruiting new employees, provide a general information session about the GDPR and their obligations with regard to personal data.

- Make this session a part of the onboarding process.

✓ Schedule regular training sessions for employees.

- Take into account their responsibilities and the nature of the personal data they come into contact with.
  they come into contact with.
- Always provide a short questionnaire or quiz after the training, and keep a precise record of both the participants and the final scores in a central overview.
- Change the (order of) the questions each time and update the content at least annually.

✓ Conduct regular awareness campaigns explaining basic principles of the GDPR and recent decisions of the DPA, among others.

- Data Protection Day (28/01)
- GDPR FAQ on the intranet

Questions?