privacy perfect

PRIVACY COMPLIANCE

Information security and the handling of personal data breaches

With Annemarie Vervoordeldonk and Noortje Molenaar

YOUR HOSTS

Annemarie Vervoordeldonk
annemarie@privacyperfect.com

Noortje Molenaar
noortje@privacyperfect.com

privacy perfect

PRIVACYPERFECT IN BRIEF

◉

Legal-tech scale-up, founded in 2015

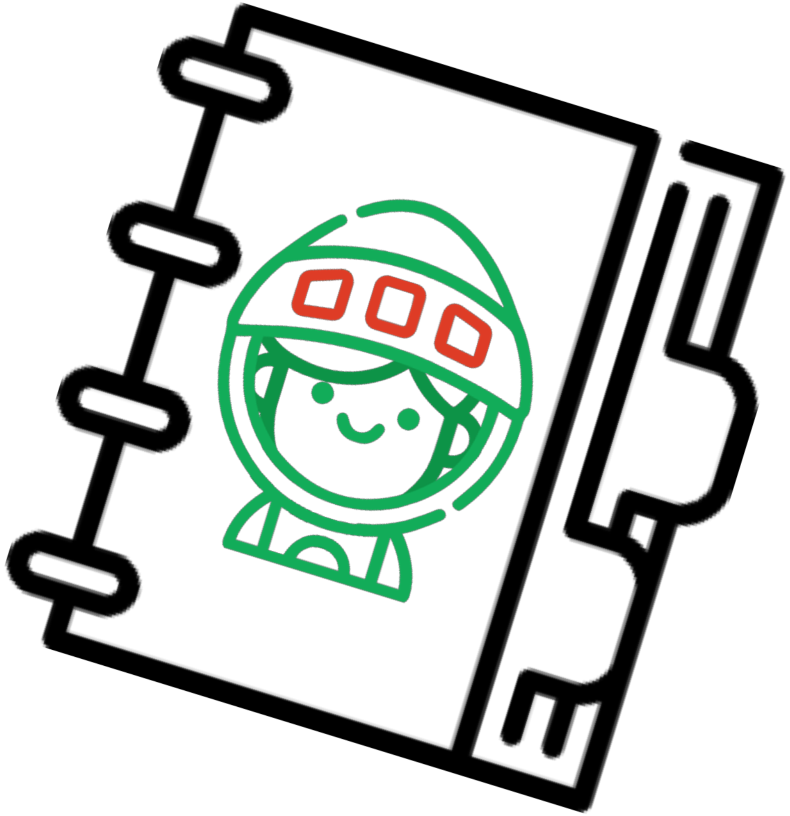
◉

Serving an **international market**

◉

Simple. Compatible. Efficient.

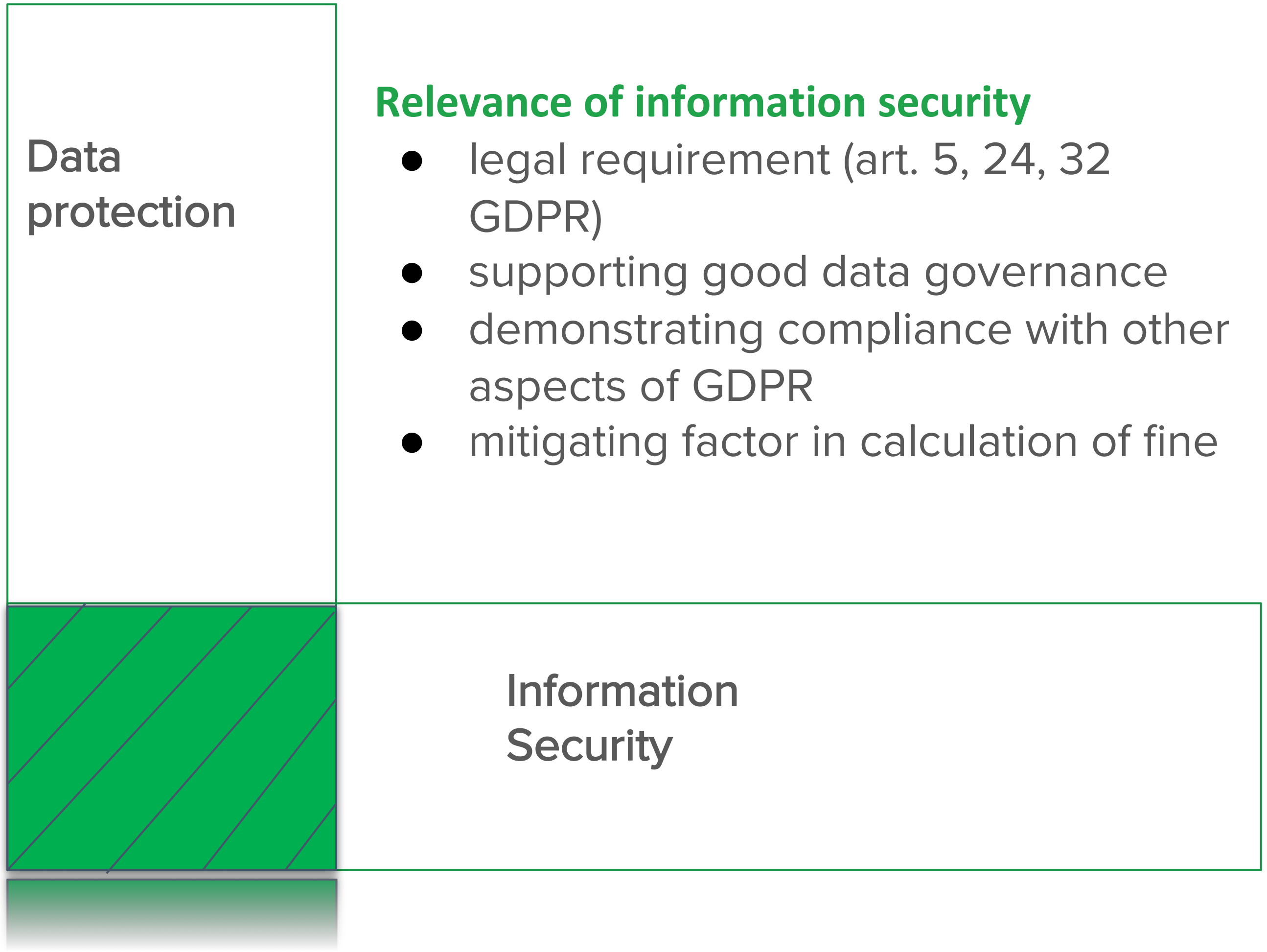
AGENDA FOR TODAY



1. Welcome & introduction
2. What is a data breach?
3. To notify or not to notify
4. What to do when an incident occurs
5. Commonly experienced challenges
6. Tips for setting up and maintaining a data breach register
7. Data breaches and automation
8. Closing & questions

privacy perfect

DATA PROTECTION – INFORMATION SECURITY

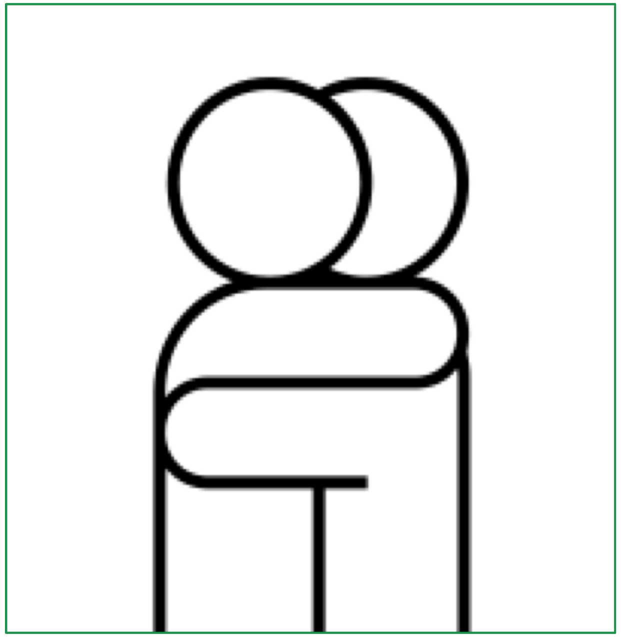


Data protection

Relevance of information security

- legal requirement (art. 5, 24, 32 GDPR)
- supporting good data governance
- demonstrating compliance with other aspects of GDPR
- mitigating factor in calculation of fine

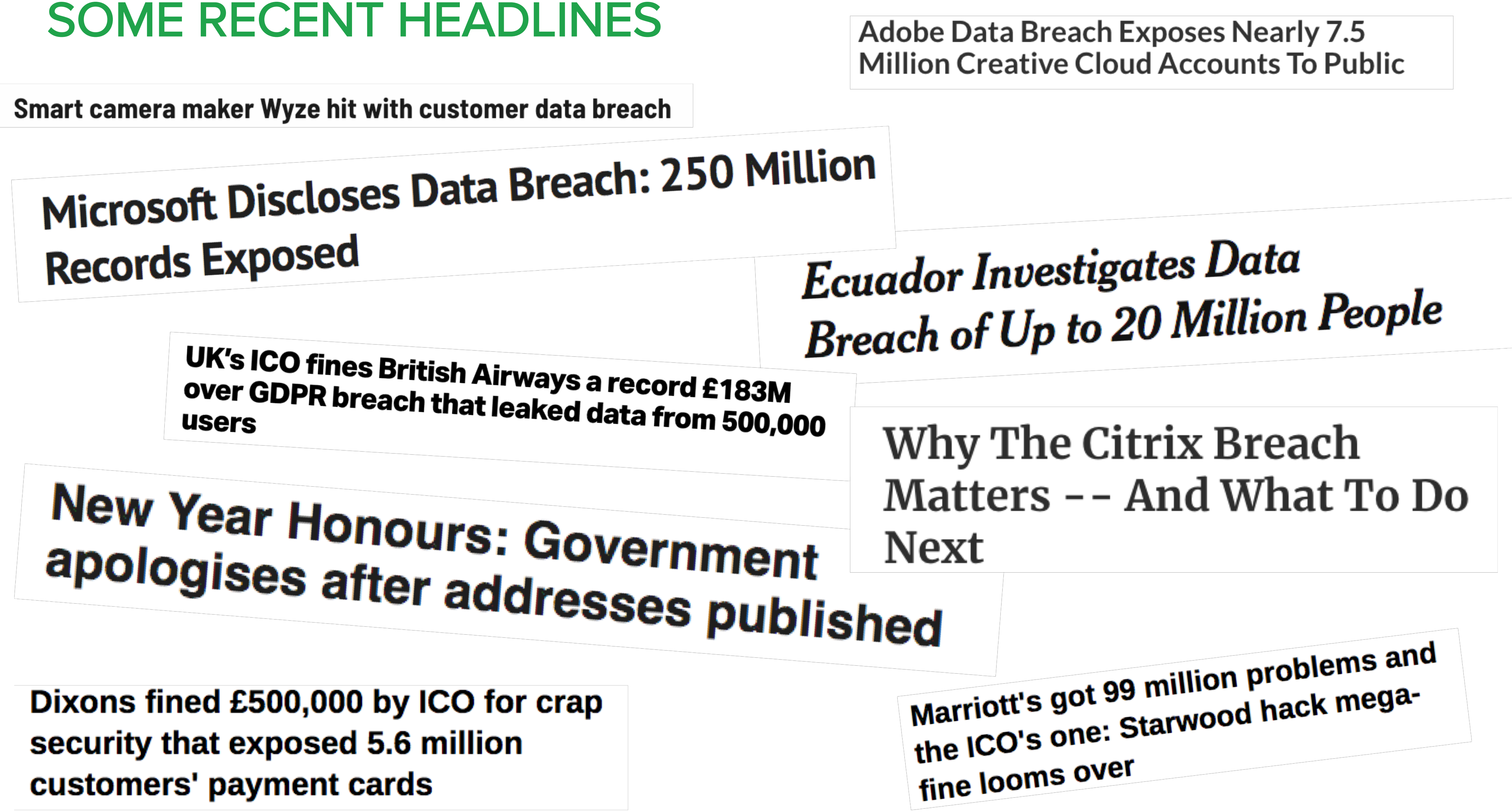
Information Security



TERMINOLOGY

- Personal data
- Accountability principle
- Controller
- Processor
- EDPB (WP29)

SOME RECENT HEADLINES



Adobe Data Breach Exposes Nearly 7.5 Million Creative Cloud Accounts To Public

Smart camera maker Wyze hit with customer data breach

Microsoft Discloses Data Breach: 250 Million Records Exposed

Ecuador Investigates Data Breach of Up to 20 Million People

UK's ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users

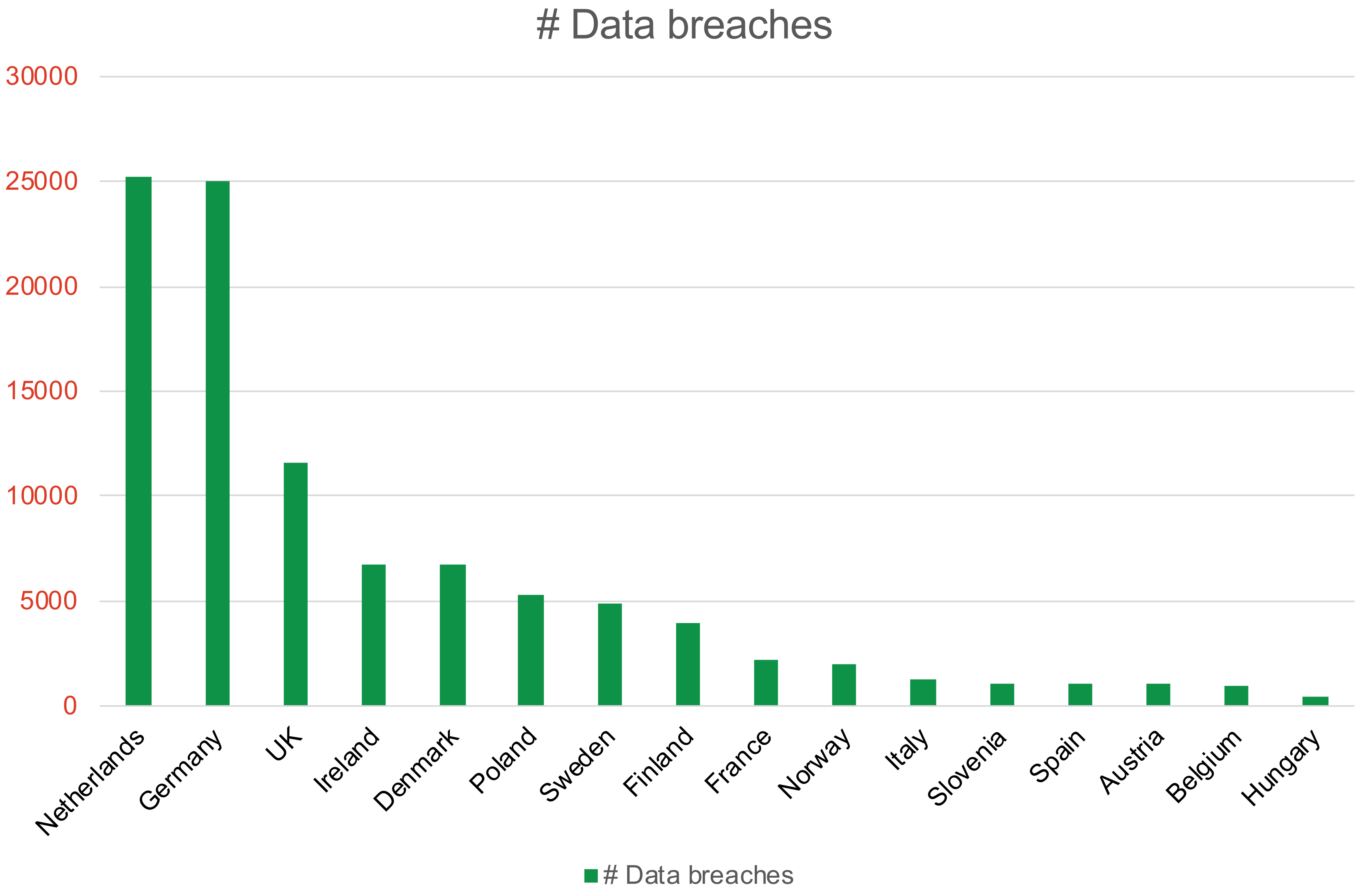
Why The Citrix Breach Matters -- And What To Do Next

New Year Honours: Government apologises after addresses published

Dixons fined £500,000 by ICO for crap security that exposed 5.6 million customers' payment cards

Marriott's got 99 million problems and the ICO's one: Starwood hack mega-fine looms over

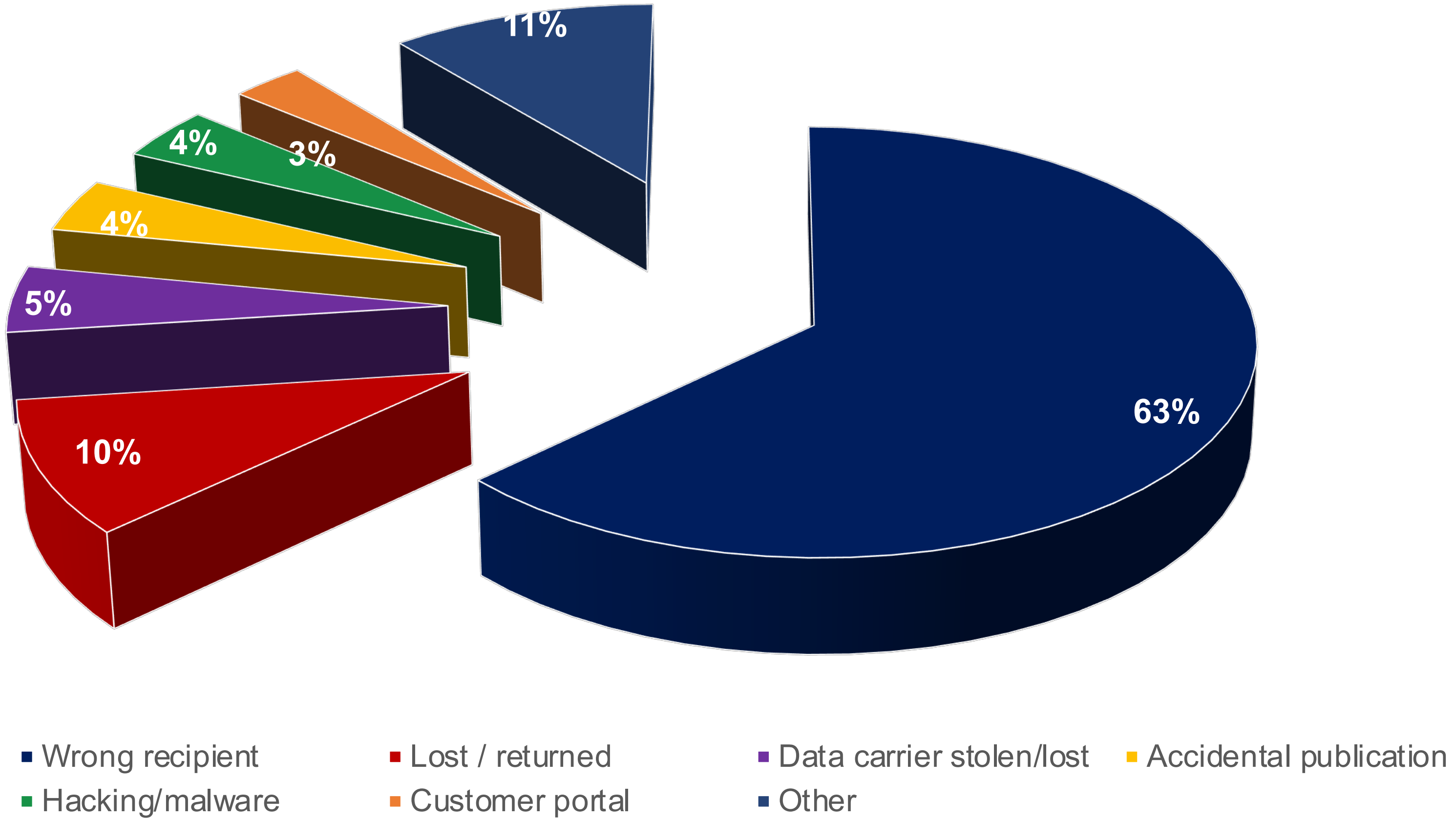
Data breaches january 2019 – january 2020



privacy perfect

Source : DLA Piper GDPR data breach survey: January 2020

TYPE OF DATA BREACHES IN NL IN FIRST HALF OF ‘19



Source: Meldplicht datalekken: facts & figures first half 2019 (Autoriteit Persoonsgegevens)

Not all cyber crime...

The 41st International Conference of Data Protection and Privacy Commissioners:

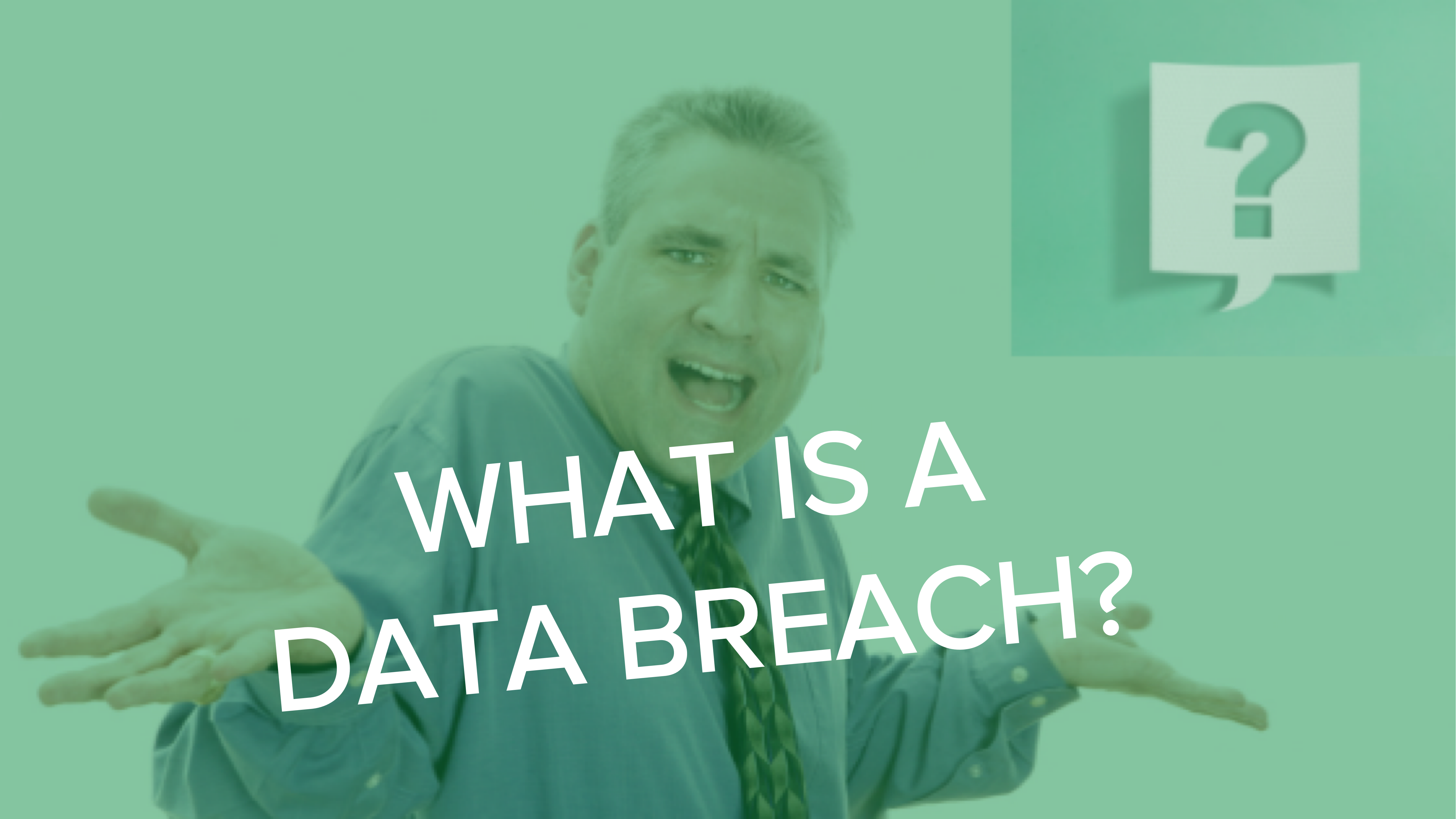
[...]

HIGHLIGHTING that notifications of personal data breaches and regulatory action in some member jurisdictions as well as national and international studies show that personal data breaches often involve **human error**, specifically **employees unintentionally disclosing personal data** to unauthorised recipients or individuals being deceived into **compromising user credentials** that allow access to information and systems ("**human error**")

[...]

have adopted a resolution to address the role of human error in personal data breaches.

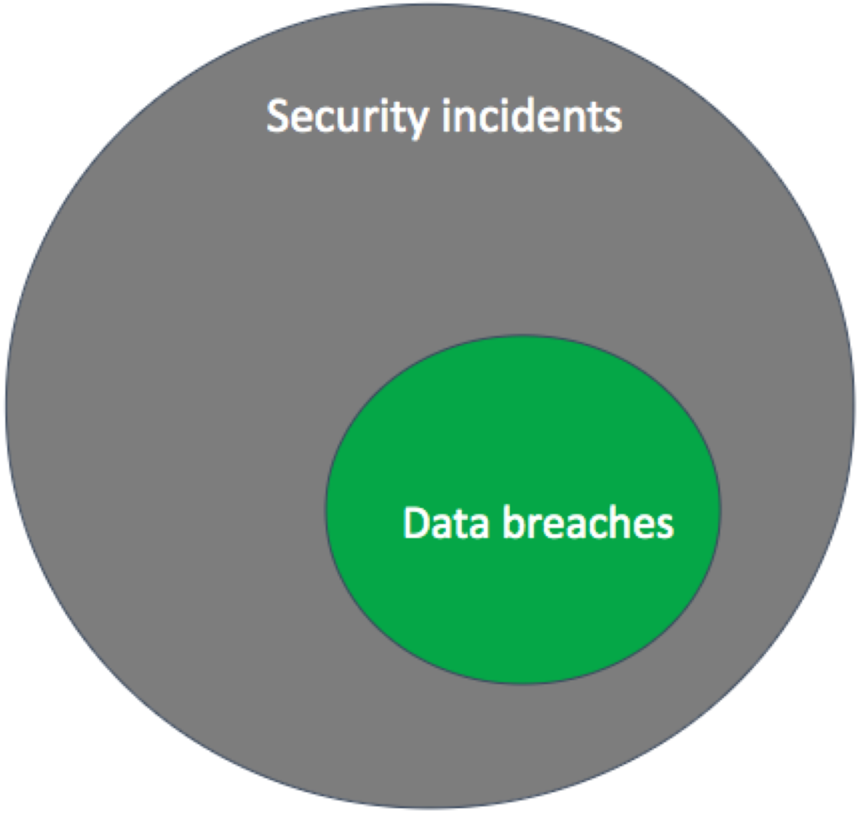
October 2019 (Tirana, Albania)



WHAT IS A DATA BREACH?

DEFINITION DATA BREACH

“A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”
(Article 4 GDPR)



Key element of any data security policy: being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner

‘APPROPRIATE’ SECURITY MEASURES

- Depends on the circumstances
  - Appropriate to the risks
  - State of the art
  - Costs of implementation
  - Nature, scope, context, purpose of processing
- No ‘one-size-fits-all’ solution
- Available guidance
  - Guidelines from EU supervisory authorities
  - Different frameworks: COBIT, AICPA, NIST, ENISA, NOREA…
  - ISO 27001 + ISO 27701

GDPR has adopted
a risk-based
approach

TYPES OF DATA BREACHES

CONFIDENTIALITY BREACH

INTEGRITY BREACH

AVAILABILITY BREACH

CIA

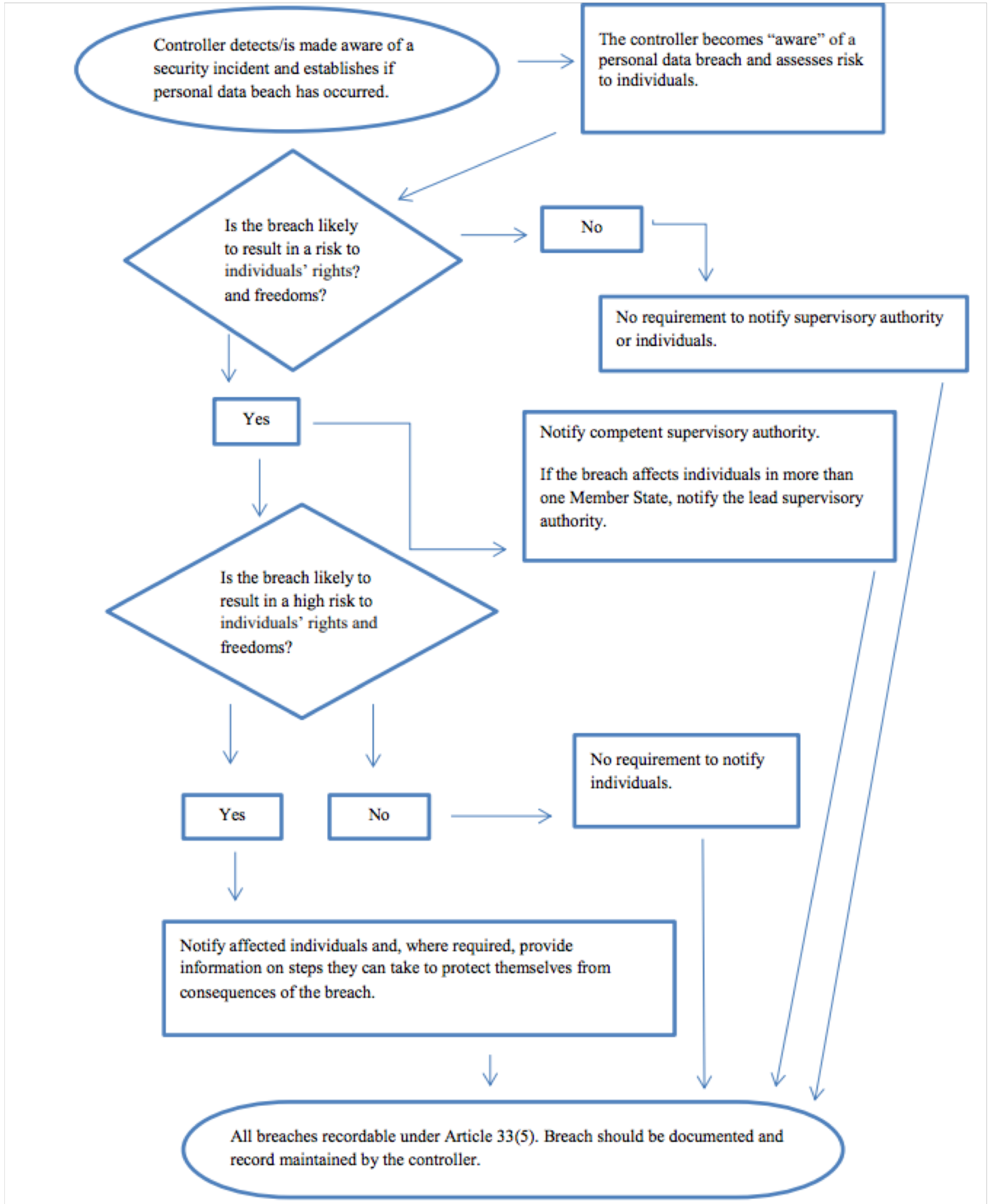
Impact on rights and freedoms of individuals

Scope of impact or ‘risk’ concept is wide:

- Charter of Fundamental Rights of the European Union
- Any significant economic or social disadvantage to natural persons - physical, material and non-material
- Examples:
  - limitation of rights of individuals (access, erasure, correction etc.)
  - identity theft or fraud
  - financial loss
  - reputational damage
  - loss of confidentiality of personal data protected by professional secrecy
  - discrimination
  - loss of control over personal data

privacy perfect

TO NOTIFY OR NOT TO NOTIFY?



Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.

The controller becomes "aware" of a personal data breach and assesses risk to individuals.

Is the breach likely to result in a risk to individuals' rights? and freedoms?

No

No requirement to notify supervisory authority or individuals.

Yes

Notify competent supervisory authority.

If the breach affects individuals in more than one Member State, notify the lead supervisory authority.

Is the breach likely to result in a high risk to individuals' rights and freedoms?

Yes

No

No requirement to notify individuals.

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.

All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

Source: Guidelines on Personal data breach notification under Regulation 2016/679 (WP29/EDPB 6 February 2018)

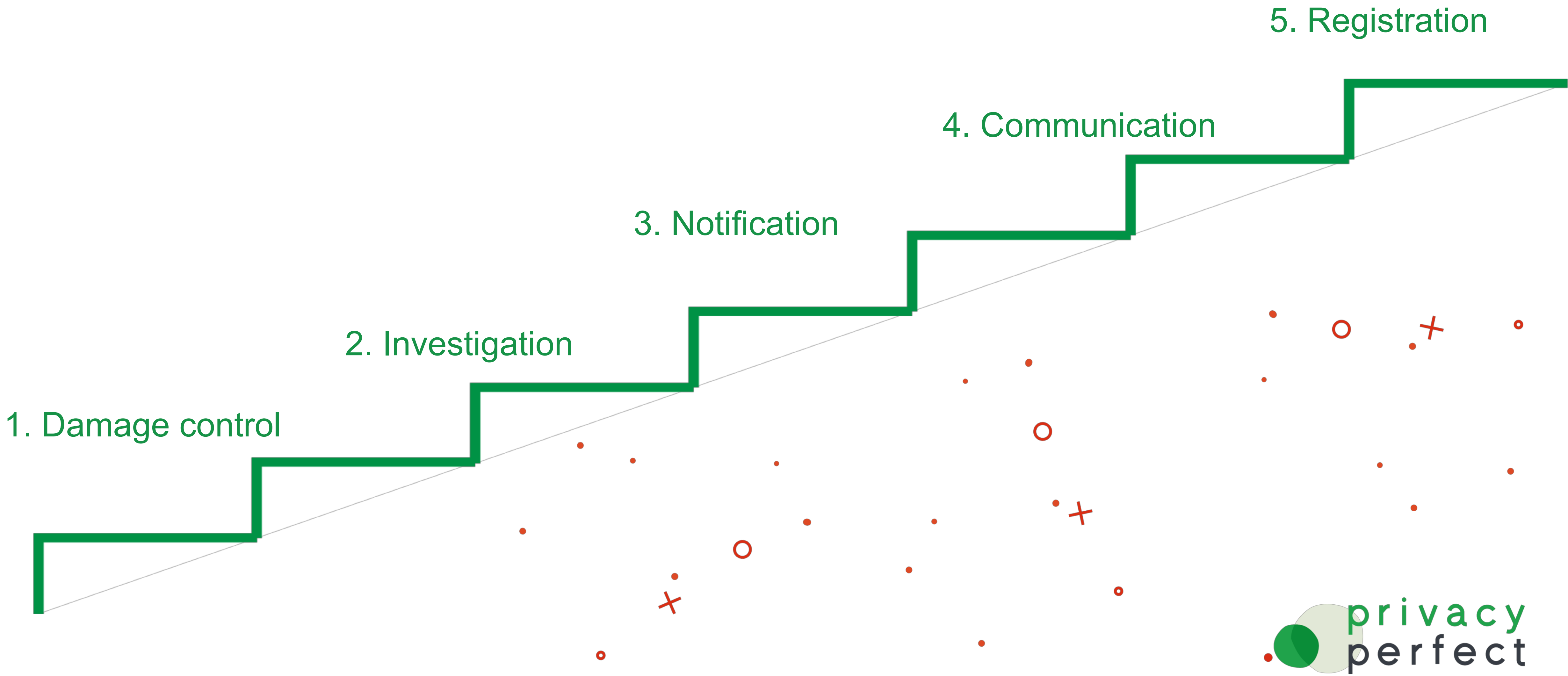
WHAT TO DO WHEN AN INCIDENT OCCURS

Too Late!

PREPARATION

- Set up data breach procedure
- Determine lead supervisory authority
- Create an internal notification point
- Form a data breach response team
- Organize awareness sessions
- Simulate a data breach

STEPS TO TAKE IN CASE OF AN INCIDENT



1. Damage control
2. Investigation
3. Notification
4. Communication
5. Registration

privacy perfect

COMMONLY EXPERIENCED CHALLENGES

privacy perfect

CHALLENGES

- Internal data breaches
- Cross-border breaches
- Coping with different reporting requirements
- Taking the lead in joint-controllership
- Delayed notification

privacy perfect

TIPS FOR SETTING UP AND MAINTAINING A DATA BREACH REGISTER

privacy perfect

TEN TIPS FROM THE DUTCH SUPERVISOR

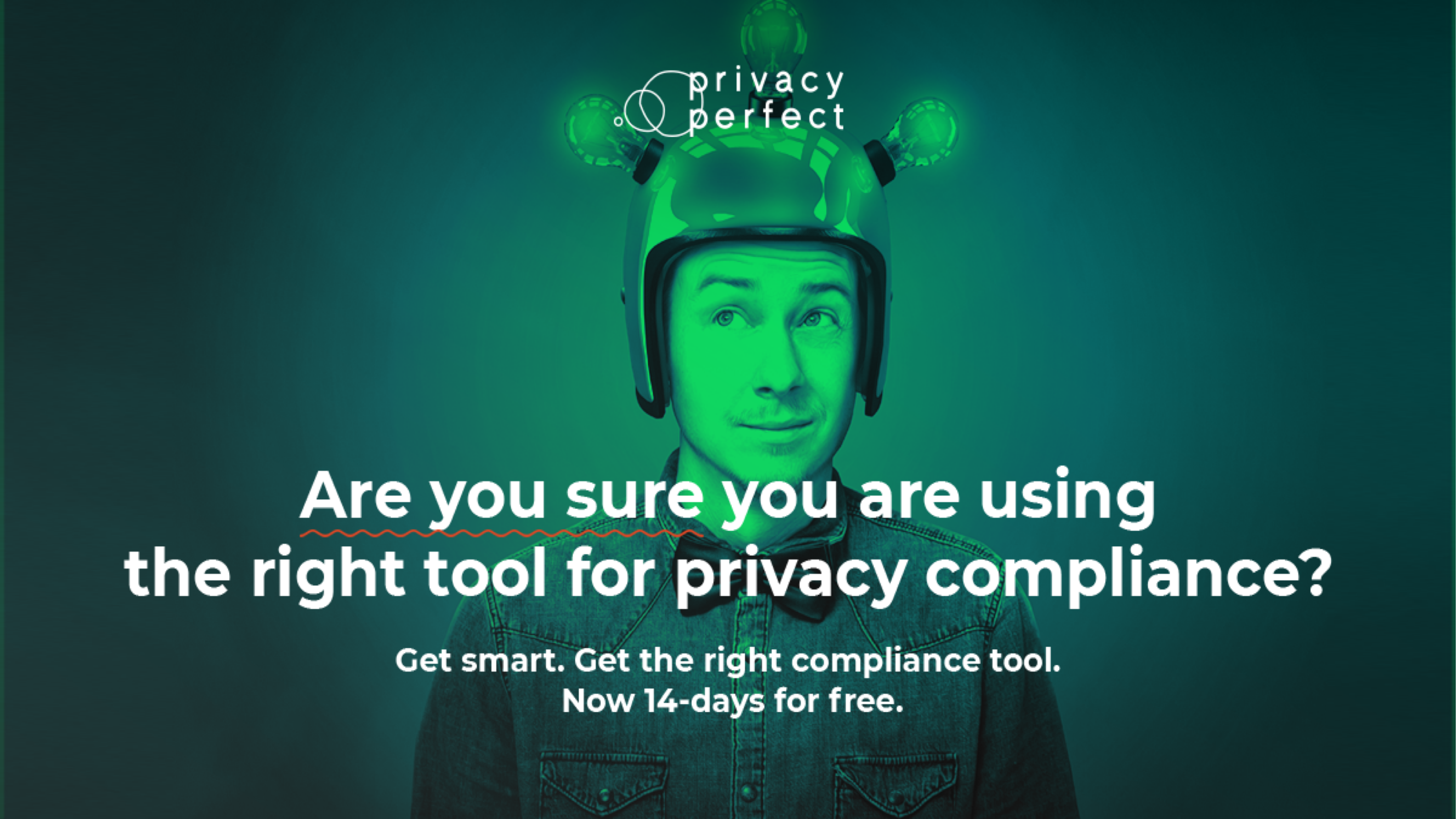
1. Provide a clear and complete description of incidents, consequences and corrective measures.
2. Distinguish explicitly between corrective and preventive measures.
3. Set up one data breach register, with the same levels of detail for each department in the organization.
4. Indicate for each incident if the data protection officer (DPO) is involved - and in what way.
5. Indicate for each incident if it has been notified to the supervisory authority and the data subjects - and explain why.

TEN TIPS FROM THE DUTCH SUPERVISOR

6. Be transparent towards persons involved if a data breach has occurred. Communicate efficiently and timely. Retain evidence of this in your data breach register.
7. Make a manual or provide training to employees who fill out the data breach register.
8. Document what other organizations were involved (e.g. controllers, processors or sub-processors).
9. Consider to make a distinction between data breaches, depending on nature, consequences, data subjects and possible measures.
10. Make sure to present and discuss the data breach registration regularly at the appropriate level within your organization as part of a plan-do-check/learn-act cycle.

BREACHES & AUTOMATION

- Save time
- Use insight for prevention
- Built-in legal knowledge and reuse of information
- Traceability / versioning/ permissions etc.



privacy perfect

Are you sure you are using the right tool for privacy compliance?

Get smart. Get the right compliance tool.
Now 14-days for free.

KEY TAKEAWAYS

WORK SMART

BE PREPARED

WHEN IN DOUBT

REPORT THE BREACH

BE EFFICIENT

AUTOMATE WHERE POSSIBLE

THANK YOU!

Do you have any questions?

Contact us via:

info@privacyperfect.com
www.privacyperfect.com

privacy perfect

RESOURCES

1. Guidelines on Personal data breach notification under Regulation 2016/679 (as last Revised and Adopted on 6 February 2018)
2. Charter of Fundamental Rights of the European Union
3. ISO/IEC 27701:2019 - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management
4. NIST Privacy Framework 1.0: Manage privacy risk, demonstrate compliance
5. Resolution to address the role of human error in personal data breaches - 41st International Conference of Data Protection and Privacy Commissioners, October 2019, Tirana, Albania