DATA BREACH & SME

Prof. dr. Patrick Van Eecke
Global Co-chair Data Protection and Cybersecurity Practice
Professor University of Antwerp

Your speaker

Dr. Patrick Van Eecke is a partner with the Intellectual Property & Technology department of DLA Piper, and global co-chair of the Data Privacy and Security Group. He has more than 20 years of experience in advising clients in areas such as e-commerce, marketing, data protection, IT, telecom and e-signatures.

He is extensively involved in diverse consulting projects for the European Commission, national governments and multi-national global corporations.

Patrick is a professor at the University of Antwerp, teaching European Information and Communications Law. He is also a guest lecturer on Internet law at various universities, such as Solvay Business Institute, Kings College London and Queen Mary University of London.

Some recommendations:

- Highly commended for the firm's Privacy "GDPR" client offering (FT Innovative Lawyers Awards 2018)
- Listed as Acritas Star™ Lawyer 2017 (Acritas Star Lawyers' report 2017)
- Awarded Best Law Firm of the Year (Trends Legal Awards 2017)
- Awarded Best IT, IP and TMT Law Firm of the Year (Trends Legal Awards 2017)
- Commended for Client Service (Chambers Europe Awards 2016)

Partner, Brussels
Global co-chair of the Data Privacy and Security Group

T: +32(0)2 500 16 30
M: +32 475 68 06 76
patrick.vaneecke@dlapiper.com

Education

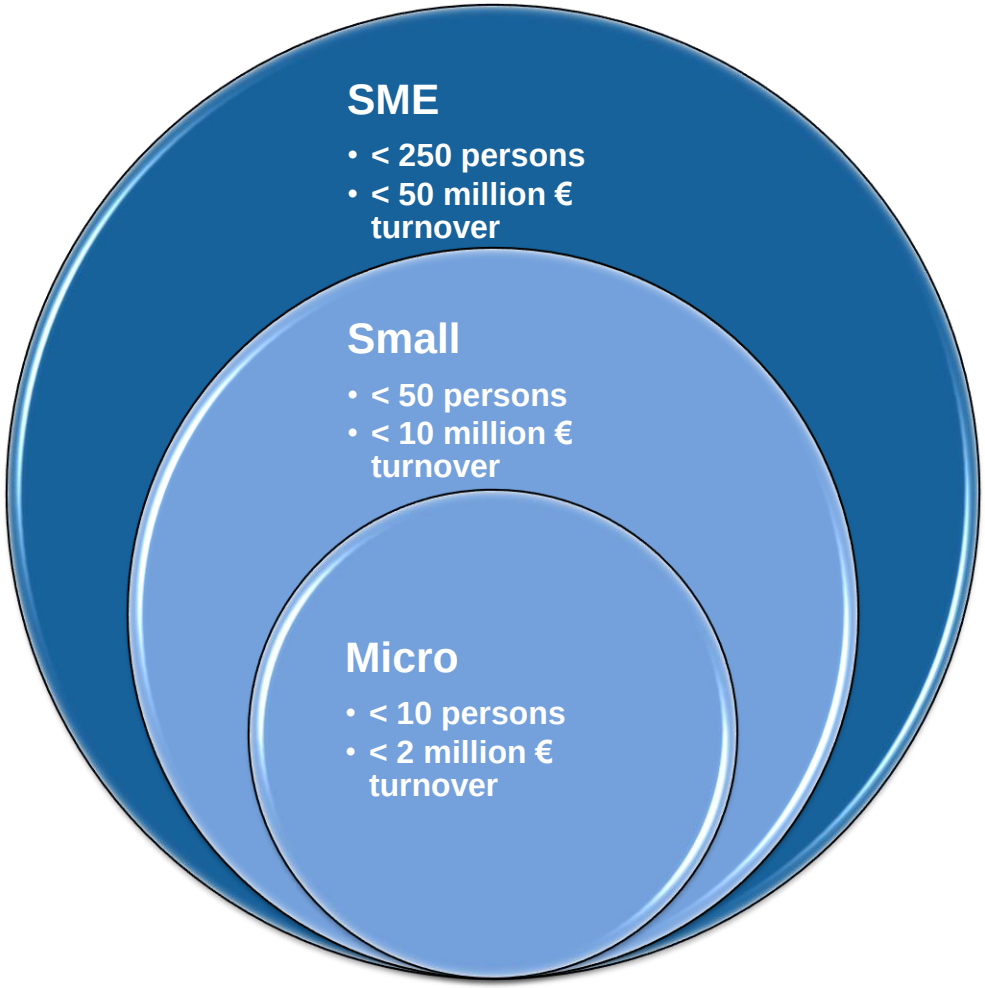
Harvard Business School Leadership for professional services firms; KU Leuven – PhD; Stanford University – research fellow; LL.M. Universität Trier; Law degree KU Leuven; Law degree Université de Rouen.

Admissions
Member of the Brussels Bar (since 1994)

Languages
Dutch, English, French

Definition of a SME

- Commission Recommendation 2003/361/EC
  - Enterprise: any entity engaged in an economic activity, irrespective of its legal form
  - E.g. self-employed persons, family businesses, partnerships or associations.



The DNA of a SME

Focus on business, less on risks

Tackle the issues when they arrive

Compliance is a cost

DIY mentality ("I can do!")

No in house counsel or "generalist" in house counsel

No DPO or just formal appointment

Discussing data breach with SME's

GDPR, is that not meant to regulate Facebook, not us?

Don't worry, we will take care of it when it comes

I will take care of it, I also handle IT and finance

It will never happen to us, we are a small fish in the pond

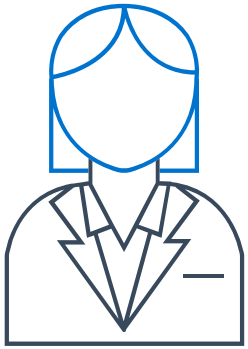
We do not process personal data

Please no procedures or handbook, we are a SME

Busy, busy, busy!

But I finally found the time to join a seminar on GDPR.

GDPR has no secrets for me any longer !



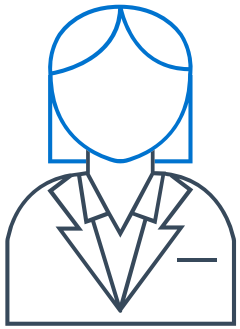
CFO

Good morning Lydia, I think I lost my USB stick with our customer data yesterday evening in the train.

Sales manager

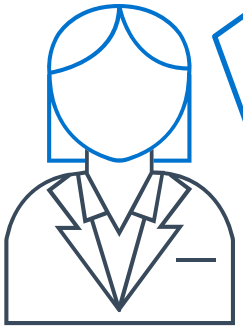
Hmm,Jamie, that sounds like a data breach.

We should investigate this!



CFO

Help, a data breach!



CFO

I have a data breach if "…" ? So, even the loss of a USB stick?

I need to inform DPA without *'undue delay'* after "*I became aware of it*"?

But wait, I do not need if "*unlikely to result in*"? What does that mean?

If I don't notify, turns out I am wrong about "*unlikely*" --> sanction up to 2%

So, I better notify the loss of my usb stick?

But which DPA should I notify, it was lost on the train from Paris to London?

Oh, but I also need to notify the people, if "*likely to result in a high risk*"? What the heck is a high risk?

But not if it does "*not materialize*"?

I am lost. Can't we just keep it under the radar screen, nobody will know

Panic & lost in GDPR lingo

Result: Once a cyber incident occurs: how SME reacts?

Based on gut feeling

- Do nothing: It will go away
- Panic: Overreact and notify everything by default, bad press communications

Results in

- Non-compliance
- Increased risk for data subjects
- Reputation risks

How can we help SMEs to better prepare themselves?

Don't believe SME's will change their SME mentality

Create awareness and provide training

Provide clear guidelines using practical rules of thumb

Provide self-service tools that can be used by non-experts

Building a plan based on 3 pillars

I. PREPARE

- **Invest in prevention**! Build Cyber resilience by investing in information security measures and applying the rules throughout the company
- Train the team before it happens in real: engage in a "**Table top exercise**"
- Check if you cyber incidents are covered by your insurance. Consider getting a **cyber insurance**
- **Review your 3rd party contracts**, because you probably work with many service providers actings as processors
- Create a **one pager** rules of thumb in case of cyber incident, just like you have in case of fire, or other incidents
- **Already engage with specialist support services** (a law firm, forensics firm and PR firm) so that in case of breach one phone call would suffice to get started

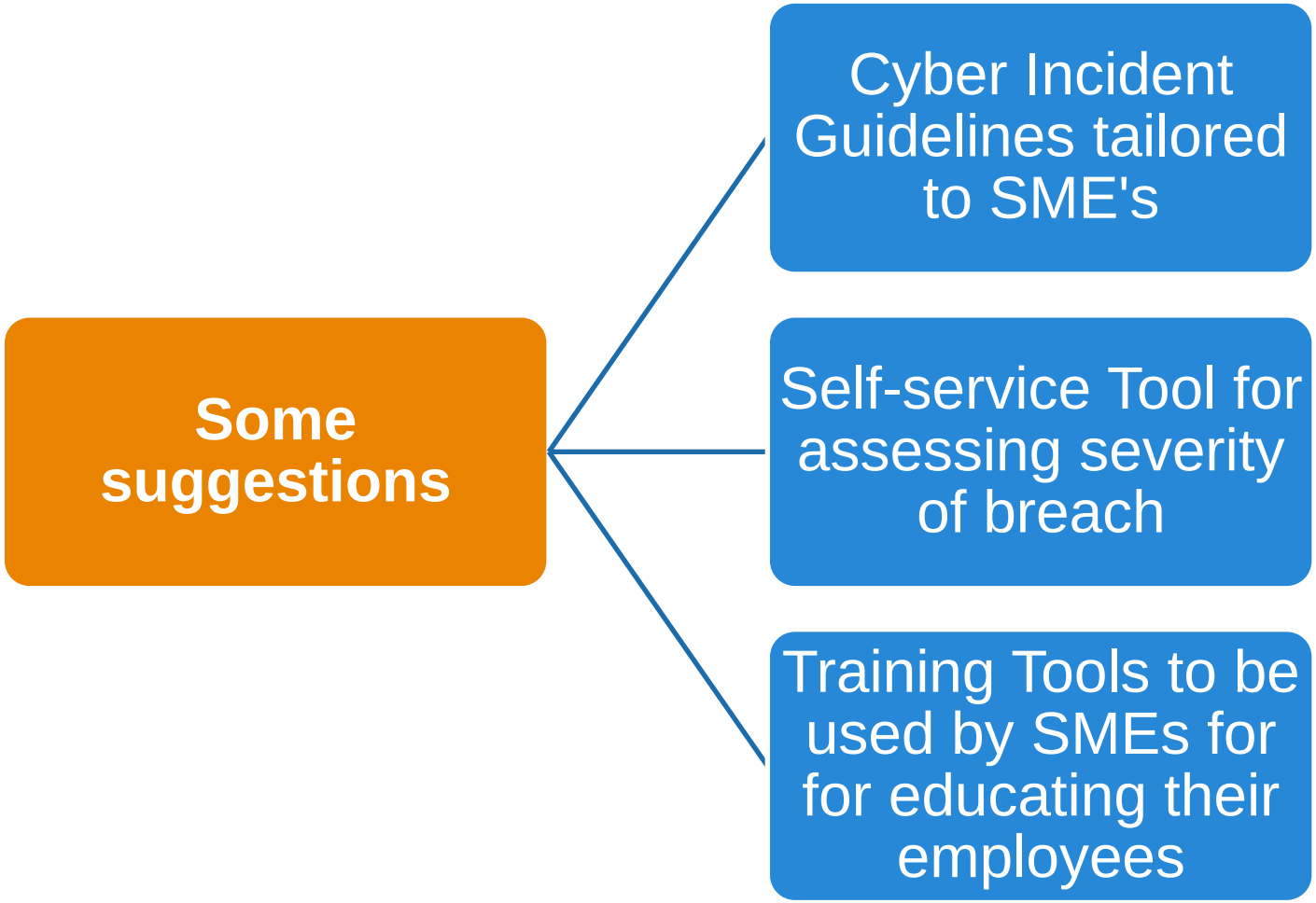
II. ACT

- Assemble **incident response team** with all relevant stakeholders.
- Instruct staff **not to speculate or discuss** the incident in writing, on social media or with the press.
- Set up a **communications workstream** and avoid the temptation to reassure when you don't know the facts.
- Set up an **investigation workstream** using forensics and legal teams to ensure the right focus and to maximise privilege. Control document creation.
- **Preserve** computer logs (stop automatic overwrite) and secure evidence.
- Set up a **notification workstream** to determine which regulators, individuals and law enforcement agencies need to be notified in which jurisdictions (and what must be notified and how). Notification deadlines are extremely short.
- Check which **insurance** is likely to engage and notify insurers. Maintain a log of losses arising and ensure compliance with terms of the policies.
- Keep a **detailed log** of the incident, investigation and response documenting the decisions taken as this may be required as evidence for regulators, claimants and other stakeholders.
- Require staff and customers to **change passwords**. Consider offering credit and fraud monitoring services (which may be a legal requirement in some jurisdictions).
- Set up **regular pulse reports** to management and staff and customers.

III. AFTER CARE

- Deal with potential **third party claims**
- Respond to **investigations** / enforcement action by data protection or other interested regulatory authorities
- Formal legal **action against** third parties who may have contributed to the incident, eg vendors or employees breaching contract terms / codes of conduct
- **Post incident review** - lessons learned, gap analysis, adopt technical and organisational improvements

Enisa: important role to play




DLA PIPER