The Perfect Storm
When Cyber-attacks Meet GDPR

Link to presentation: https://www.eugdpr.institute/Berlin/

9th November 2018

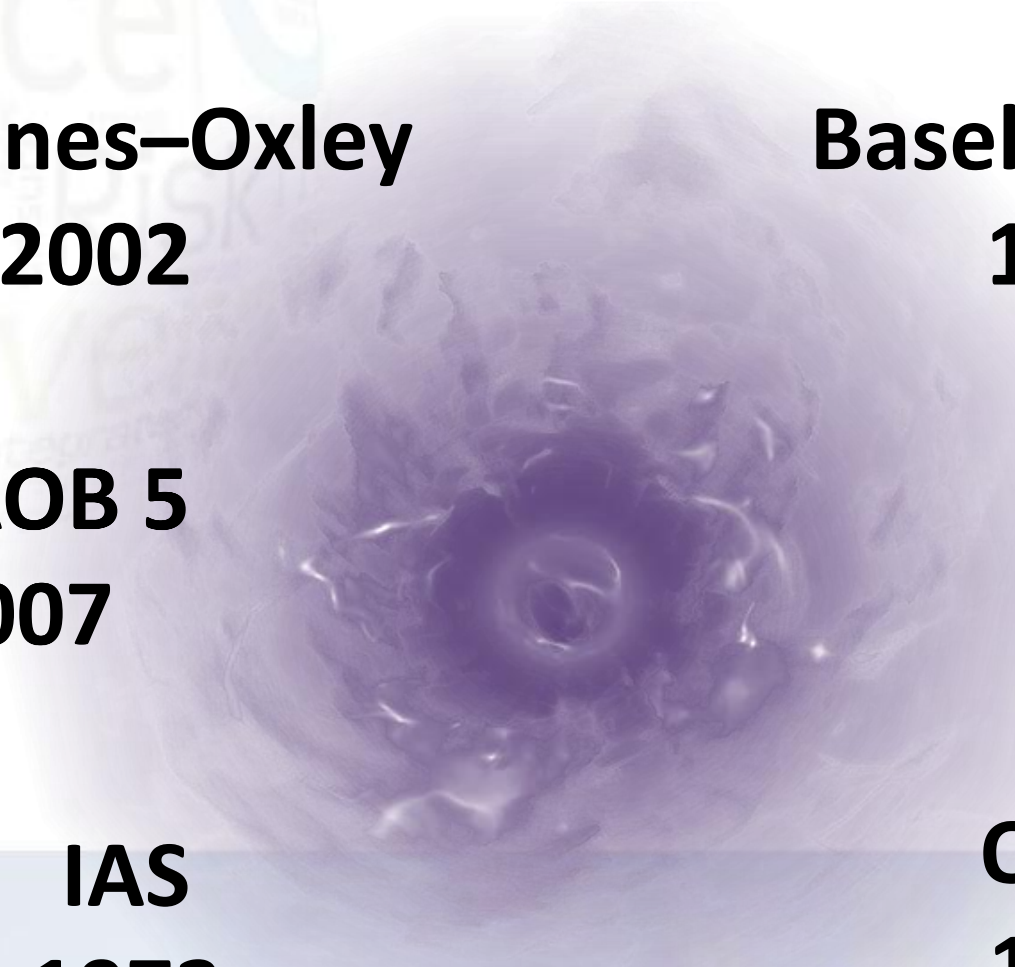
Agenda

The Perfect Storm
When cyber-attacks meet GDPR

- **How to navigate a data breach under GDPR**
- **Contents: recommendation of steps for different scenarios, selecting data recovery tools**
- **Tips for controls and policies on personal data security, and ideas for compliance preparation**

9th November 2018

50 years of perfect storms



Sarbanes–Oxley
2002

Basel Accords
1988

PCAOB 5
2007

FCPA
1977

IAS
1973

OFAC
1963

GDPR
2018

Navigating thru a storm or breach

Current cyber storm status

1 The EU countries with the highest number of incidents were Germany, Belgium, Great Britain and Spain.

2 Ransomware attacks; files are encrypted and are unlocked when……

3 The trades frequently targeted by hackers are financial services, manufacturing, telecom.

4 <1/3 of companies have a strong understanding of their cyber risks.

5 Less than a third regard cyber security as a “top-5 risk.”

6 EU organisations take three times longer to identify intrusions than the average among global companies

https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Threats%20UK.pdf

Navigating thru a storm or breach

Elements of a perfect storm

1. Data Analytics
2. Data Integrity
3. End to End Integration
4. IT Governance
5. Lifecycle Management
6. New Tech Trends like ransomware, phishing, Ddos attacks
7. Regulatory Trends

Navigating thru a storm or breach

One or more failures can start a storm

1. What could go wrong? How could a process fail?
2. The assets and IP that require care and oversight?
3. The intellectual or digital assets are used and constitute a key success factor? personally identifiable data, copyrights, and licenses.
4. Who has access to the systems and the activities they perform using it?
5. The vulnerable people, processes, systems, or assets?
6. What can disrupt the operations?
7. Complex, regulated and exposed activities?

Navigating thru a storm or breach

How to avoid a storm

1. Awareness Security training & education
2. Business continuity & disaster preparation
3. Cyber Security
4. GDPR and Data Protection Governance
5. Legal & regulatory issues
6. Organizational culture
7. Risk Management

Navigating thru a storm or breach

5 non-technological references

1 **Cyber security is not an IT issue**
it is a risk and management issue

2 **Employee aware ness of the principal cyber vulnerabilities**
vulnerability assessments are essential

3 **Conduct a vulnerability assessment,**
benchmark cyber protocols to a recognised standard

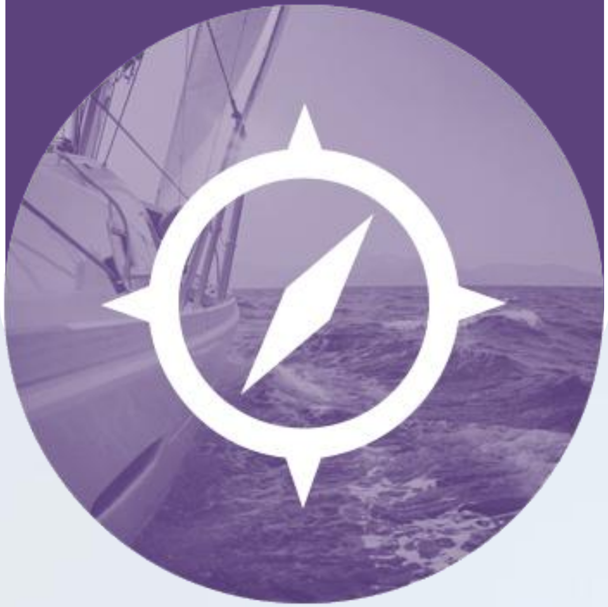
4 **Engage a top-notch security experts**
to respond to an incident

5 **Share malicious threat intelligence in real time**
promptly alerting the breached systems

Navigate a data breach

Indications of compromise

notifications from



public authorities

users

data processors and 3rd parties

data loss solutions

Navigate a data breach

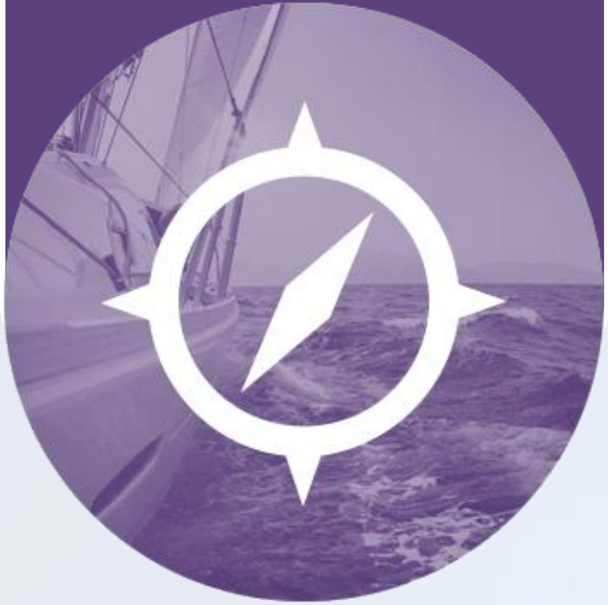
We say

"There are two types of companies: those that have been breached, and those who don't know they have been breached."

Navigate a data breach

Incident response protocol

Investigate



When occurred

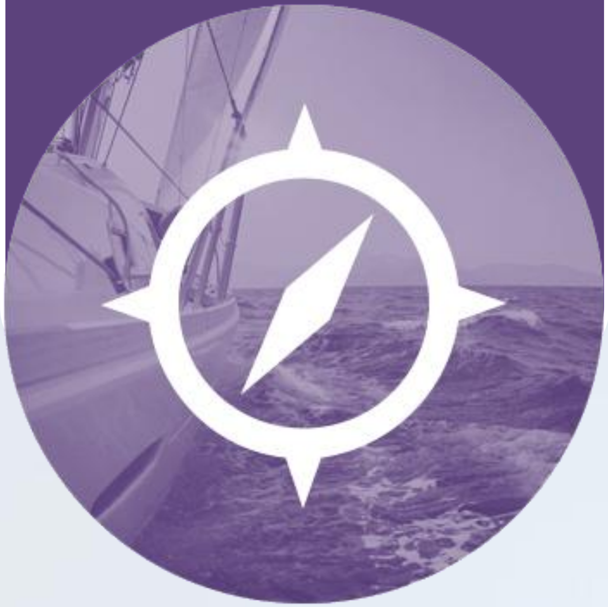
How occurred

Level of compromise

Audit the data flow

Frequent audits

Also good before implementation



Both data inflows and outflows

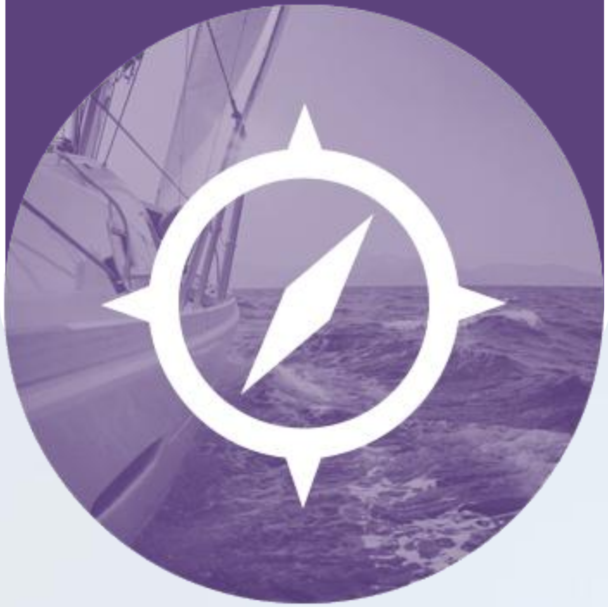
Focus on the risks of unintended uses of personal data

Ensure the RoPA is updated

Navigate a data breach

Steps

suspected or known data breach

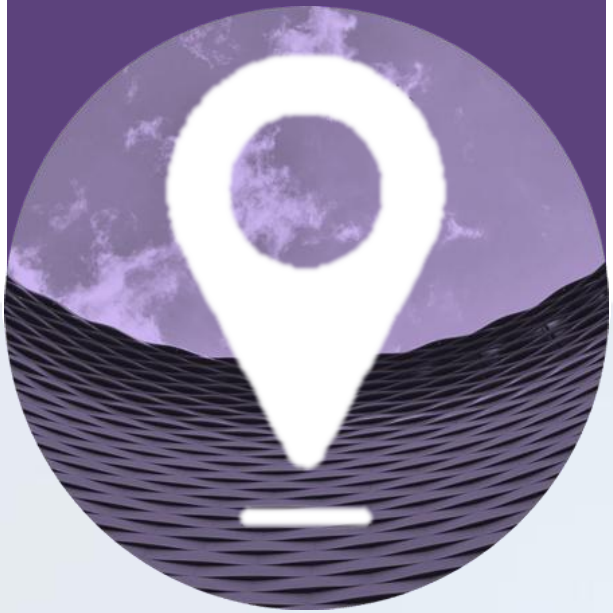


1. Contain the breach by disconnecting networks and users and revoking privileges
2. Activate the data breach response team
3. Investigate logs of suspected insiders/outsiders, preserve evidence, document &confirm
4. Assess the impact of the data loss
5. Take remedial actions: restorations, change credentials of key users and servers
6. Notify supervisory authorities and data subjects

Scenario planning

Addressing breach risks

critical data assets



Penetration testing, vulnerability scanning

Response scenarios on internal/external threats

Improve breach detection

Document prevention

Data recovery

Selecting the right tool

Internal and external factors

Compatibility

Coverage

Support

Features

Control tips

Enhancing the data governance

Invest in the RoPA

Encrypt data

Review and limit user access and activity

Protect against data leakage

Control tips

Enhancing the data governance

ISO 27001 certification for you and your vendors

Train the trainer for privacy

Assign a data owner

De-risk processes

Control tips

Enhancing the data governance

Do not confuse GDPR compliance with cyber security

Constantly assess new risks (and technological tools)

Patch timely to block vulnerabilities

Contract insurance policies

Resources

Experts. How to Prepare Your ERP System for GDPR

Learn. How to Prepare Your ERP User Access Review for GDPR

Training, awareness, workshops, certifications

Thanks

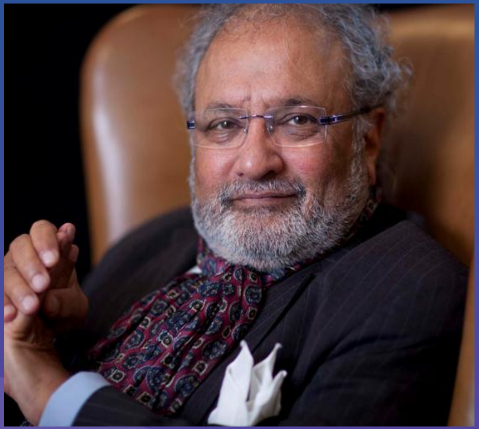
@porbunk

https://www.linkedin.com/in/kersi-porbunderwala-8760642/

GRC, GDPR, CSR, BFC and related issues

COPENHAGEN COMPLIANCE
Global GRC Solutions

EU GDPR INSTITUTE



Kersi F. Porbunderwalla is the Secretary General of Copenhagen Compliance and President of The EUGDPR Institute and Riskability IT Tools. Kersi is a global consultant, teacher, instructor, researcher, commentator and practitioner on good Governance, Risk Management, Compliance and IT-security (GRC), Bribery, Fraud and anti-Corruption (BFC) and Corporate Social Responsibility (CSR) issues. Kersi lectures at The Govt. Law College (Thrissur, India) Georgetown University (Washington) Cass Business School, (London) and at Fordham University (New York) and Renmin Law School (Beijing). Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GDPR, GRC, Risk Management ,CSR, and BFC issues.

Disclaimer: This presentation is prepared for #FODP 2018 Berlin. The content together with the links to narratives, brochures and information on our websites, is for general informational purposes only. Please refer to Copenhagen Compliance® for specific advice on regulatory compliance and other GRC issues. As always refer to your counsel for legal advise, we are not licensed to provide legal advise.

Copenhagen Compliance UK Ltd®
Info@copenhagencompliance.com
www.eugdpr.institute
21, Cloudseley Street, London N1 OHX, UK.
Tel. +91 9920801838
Tel: +45 2121 0616
Tel. +44 7778 917 13321

©The EUGDPR Institute by Copenhagen Compliance®

EU GDPR INSTITUTE

Connecting IT Security to Governance, Risk and Compliance
www.copenhagencompliance.com

Copenhagen Compliance® is the global Governance, Risk Management, Compliance and IT Security (GRC) think tank. As a privately held professional services firm, the mission is the advancement of the corporate ability to govern across the borders, sector, geography, and constituency. The primary aim is to help companies and individuals achieve integrated GRC management that unlocks the company ethics, cultures and value by optimising GRC issues to IT-Security & automation.

HR Riskability
Human Capital Assessment Framework

Copenhagen Compliance provides a global end-to-end GRC and IT security platform, with a comprehensive & proven advisory based on; giving priority to transparency, accountability and oversight issues. Our focus is on GRC Intelligence, Internal Controls, Audit, CSR, Compliance & Policy Management, IT-GRC, Sustainability Management, Bribery Fraud, Corruption , IT &- Cyber Security Issues

EU GDPR INSTITUTE

Copenhagen Compliance® has dedicated resources for consultancy and research in Good Governance, Risk Management and Compliance issues involving corporations, universities and business schools and GRC organisations on four continents. Email; info@copenhagencompliance.com Tel. +45 2121 0616

As ever, always have your legal advisors review and advise on any legal guidance or on any contractual obligation. The Copenhagen Compliance Group is neither a Law Firm nor are we licensed to provide legal advice.