

"Get Privacy": Use GDPR as Foundation Guide for Data and Analytics Prerequisites

Claudio Neiva

<50%

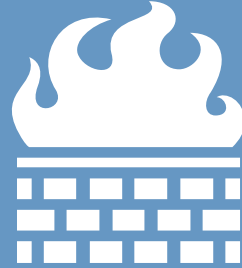
**By 25 May 2018,
less than 50% of
all organizations
will fully comply
with EU's GDPR.**



Why Should We Bother With This?



Fines. Yes. Up to 4% of global annual turnover or EUR 20M.

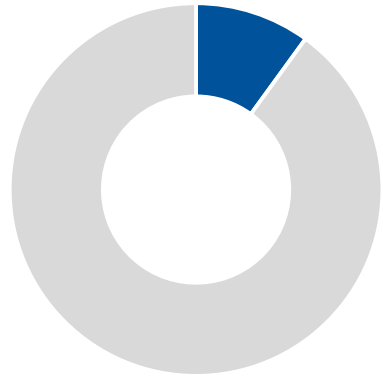


Distrusting clients and disloyal employees after breach.



Reputation and client loss when disregarding subject's rights.

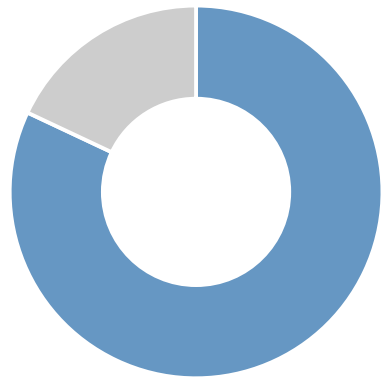
Identify the areas and processes impacted.
Assemble a multidisciplinary team to attack.



10%

of respondents believe their company is currently 100% ready for when the regulations go into effect.

Source: WatchGuard, September 2017



82%

82% of European consumers plan to exercise their new rights with respect to information collected.

Source: Pegasystems, December 2017



But there's hope:

Gartner inquiries have *skyrocketed* with **>400%**
YoY on privacy.

Source: Gartner, January 2018

Key Issues: Divide and Conquer the GDPR in Three Areas

How to Attack the GDPR:

Identify processes impacted

Assemble a team

Appoint mandated owners

Document risks



Control Your Data
Processing Activities



Communication and
Accountability Are Key



Privacy Puts the Data
Subject Prime

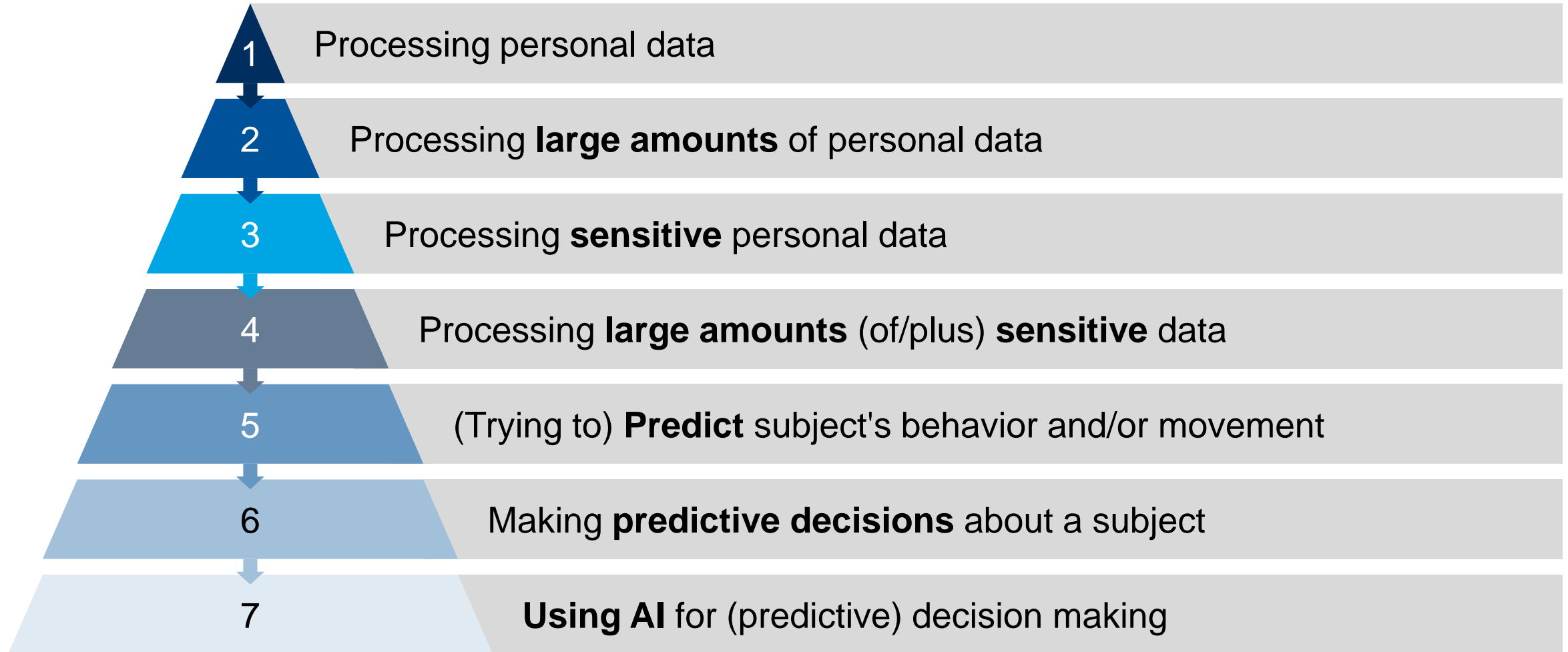
The Cost of Storing Data?



The Price of Storing Data!



Influencing Factors of Privacy Risk



Is This Your Personal Data Strategy?

You really just
don't know when
you might
need it ...



Image Credit: [TheDoctorMo](#)

Transparency and Control — Minimum Privacy Assessment

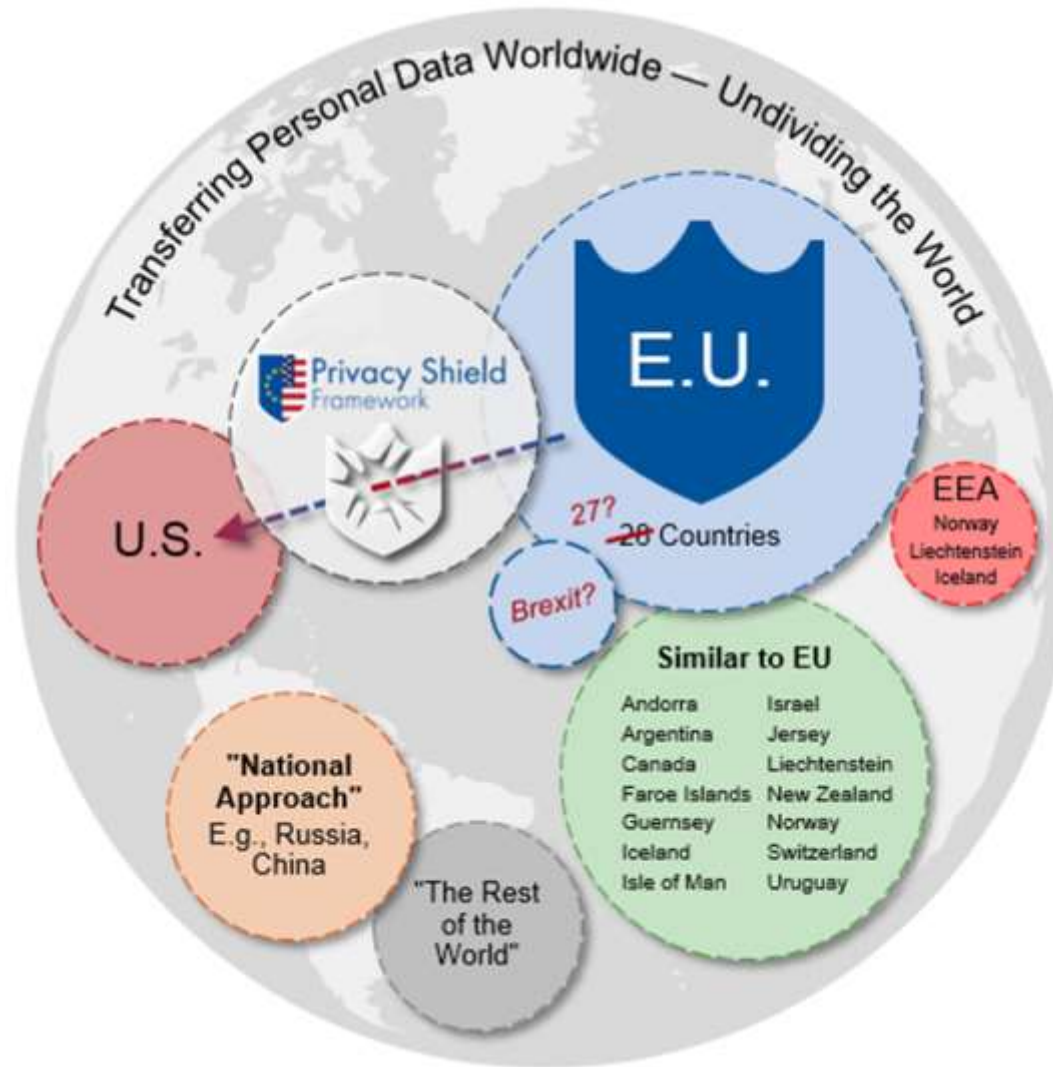
List of Personal
Data Items
Processed

List of Processing Purposes

		Indicate Use of Data per Purpose and Include Retention Periods

Describe Retention Period Trigger

Cross-Border Data Transfers — The World's a Stage



Accountability and Awareness

- Establish roles and responsibilities
- Conduct privacy impact and risk assessments — mitigate accordingly
- Bottom line: **Understand** **what** you have, **why** and **where**

Explain to your staff the importance and the road taken — **all** should be on the same page!

Key Issues: Divide and Conquer the GDPR in Three Areas

How to Attack the GDPR:

Identify processes impacted



Control:

- Identify and document processing purpose
- Document data processed
- Implement conducting PIA
- Train all key staff

Assemble a team



Communication and Accountability Are Key

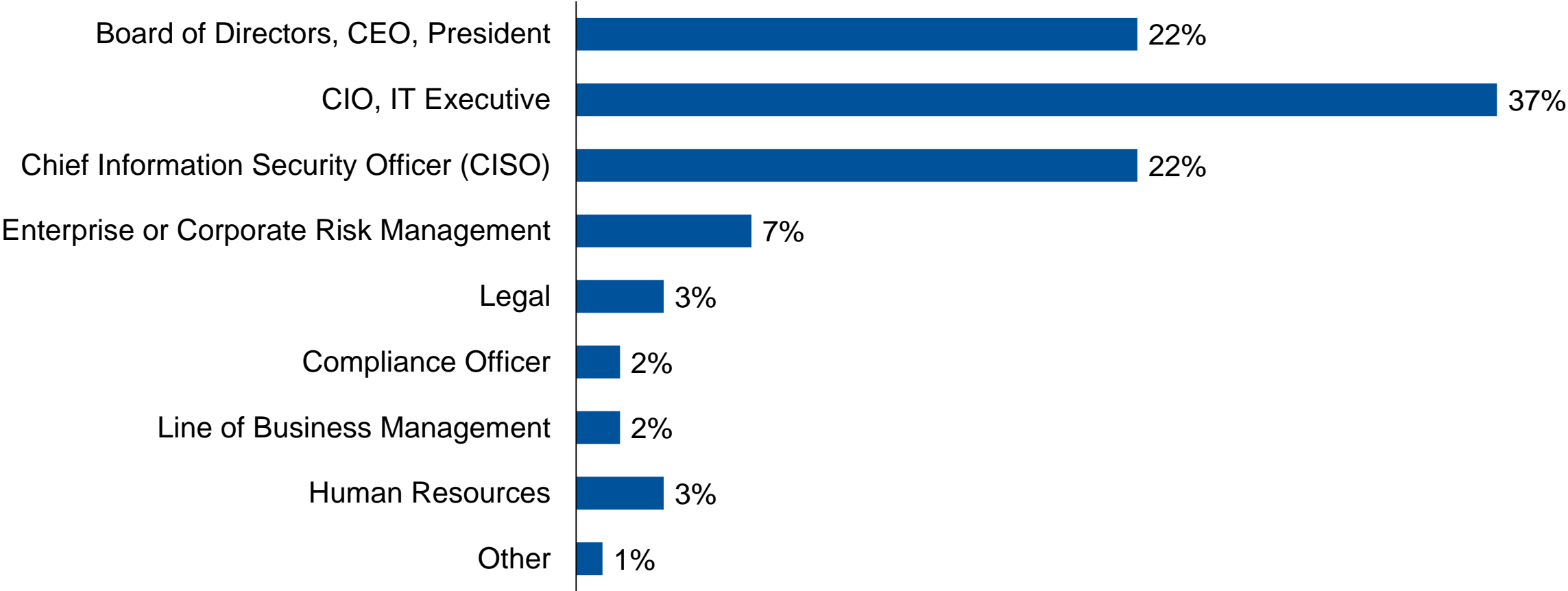
Appoint mandated owners

Document risks



Privacy Puts the Data Subject Prime

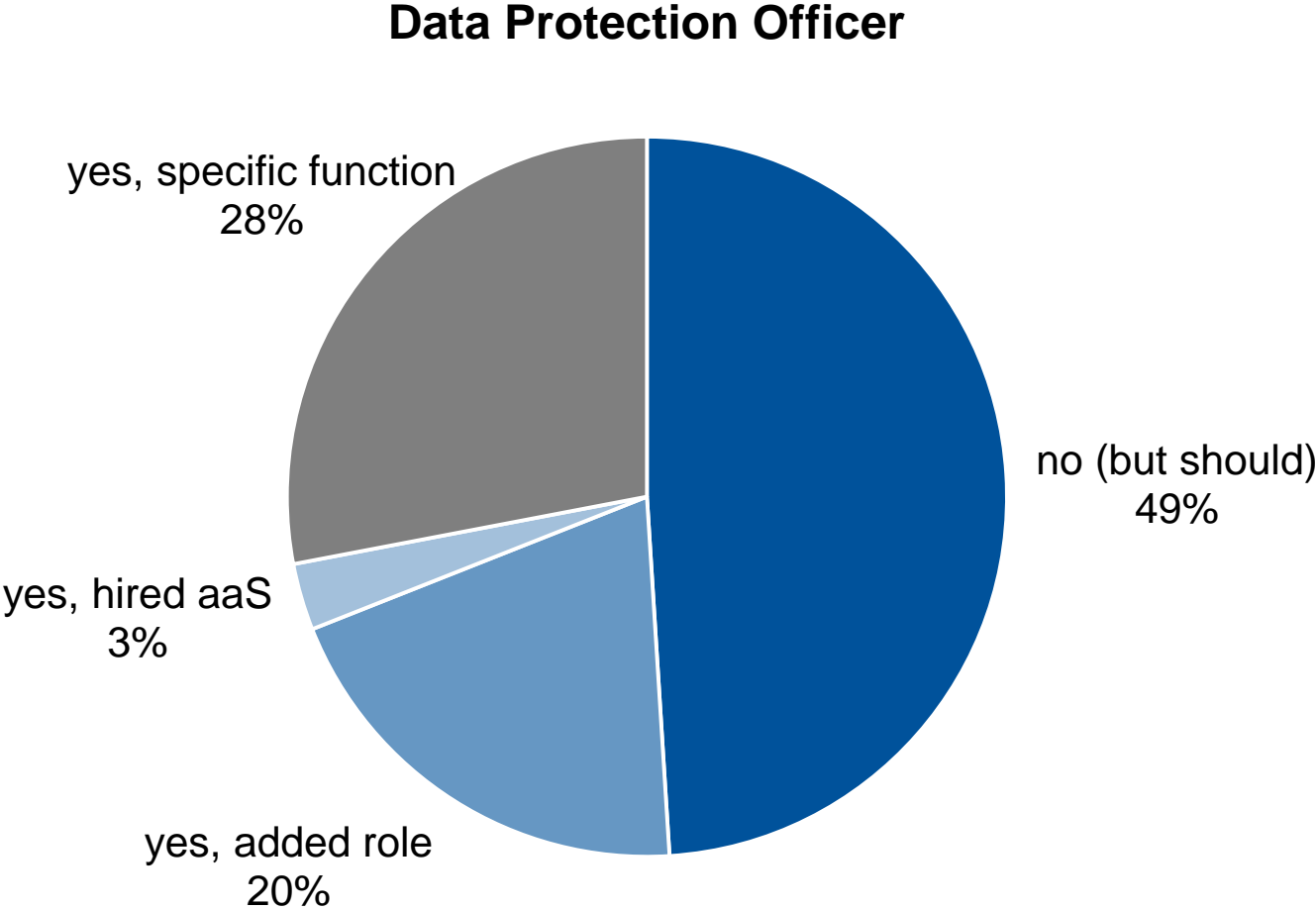
Most Senior Privacy Role Reports to ...



Percentage of Respondents

Base: Privacy, n = 286
E. In your organization, to whom does the most senior level person dedicated to privacy directly report?

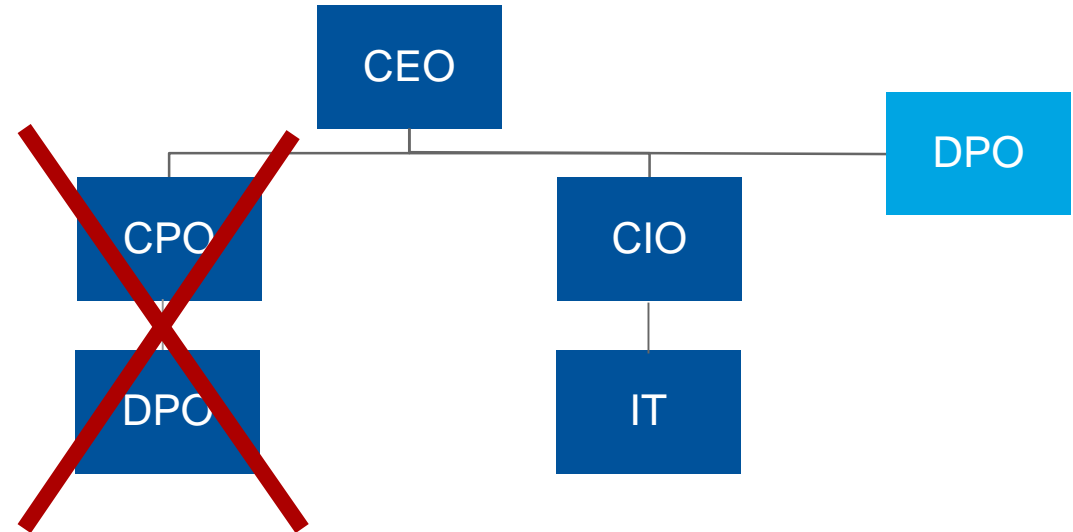
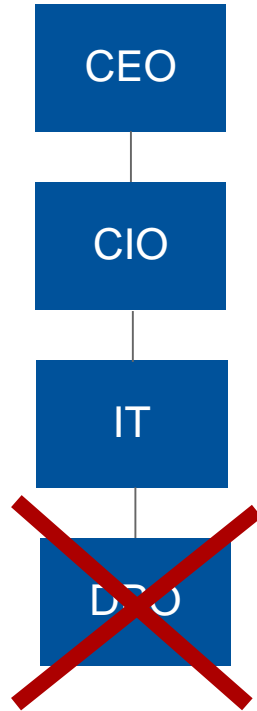
H1 2017 on the DPO



Single Point of Contact: Your DPO

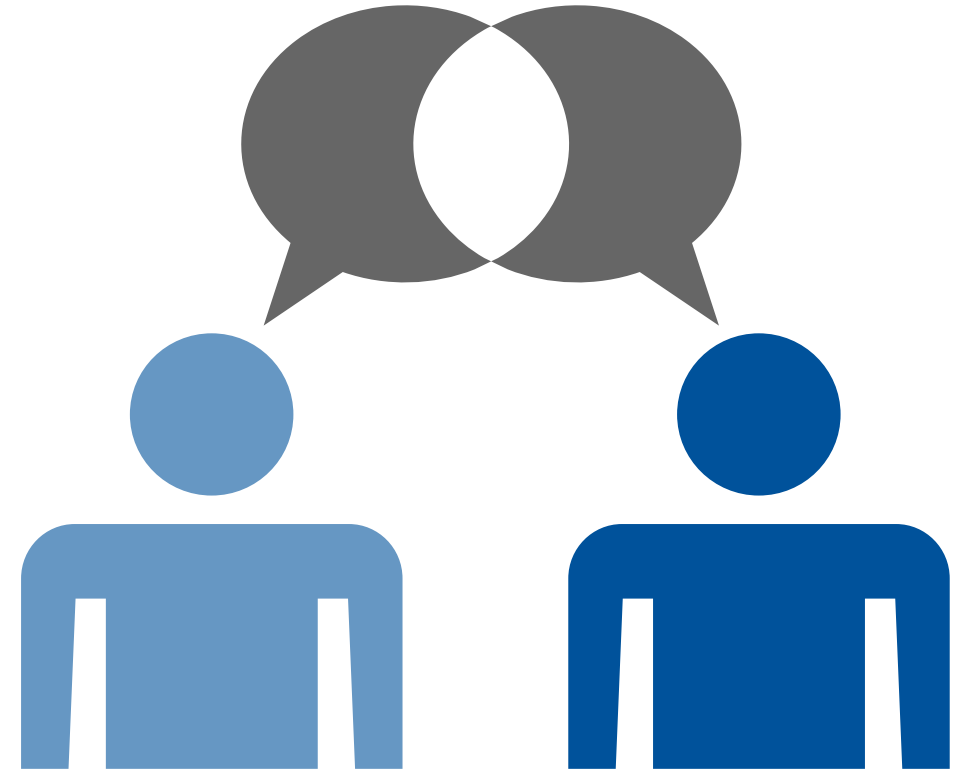
Characteristics:

- Demonstrable expert
- Independent
- Accountable?



Communication Is Key

- Your Privacy Policy and Statement:
 - For employees — full policy.
 - For subjects:
 - 6 items:
 - Who, what, why, how, who else?
 - "Contact here."




Communication Is Key

Data Breach Notification:

- Detect, investigate, respond and remedy.
- To authorities **and** the data subjects?





**There were over 750
data breaches in the
U.S. throughout 2015.**



**There were over 5500
data breaches in the
Netherlands
throughout 2016.**

Key Issues: Divide and Conquer the GDPR in Three Areas

How to Attack the GDPR:

Identify processes impacted



Control:

- Identify and document processing purpose
- Document data processed
- Implement conducting PIA
- Train all key staff

Assemble a team



Communicate:

- Appoint a DPO
- Review privacy policies
- Prepare breach notification

Appoint mandated owners

Document risks



**Privacy Puts the Data
Subject Prime**

Fines Are a Warning Signal



- Why try it out?
- The iron **will** hurt.

Remember:
GDPR = Law

- Employee and consumer

Trust

- are the fireplace!



Trust:

Takes years to build
Only one mistake to break
And **forever** to repair

93% of adults say that
being in control of
who can get information
about them is important.

— Pew Research Center, 2015

Data Subject's Rights

- The right to information:
 - Be transparent, have a good privacy statement
- Right of access:
 - Allow them to access what's "theirs"
- Right of rectification:
 - Simply right what's wrong
- Right to be forgotten (RTBF):
 - Nothing new really
- Right to restrict processing:
 - Not RTBF, but limit purposes and access
 - May require segregation of affected data from standard processing systems



12 19
1539

HB-887-G

Data Subject's Rights — Yes, There's More!

- Right to data portability:
 - A "commonly used, machine-readable format" (PDF? .csv?)
 - Easier for competition to create competing services (IPR protected information?)
- Right of notification:
 - Get those policies and statements revised and breach-process tested.
- Right to object:
 - Direct marketing, immediately.
 - "Controller's legitimate interest" likely to lose to individual privacy.
- Right not to be evaluated based on automated processing:
 - Machine learning. AI. Algorithm transparency? Bias!
- Right to bring class actions!

Data Subject's Rights

- **Prepare** to answer to these requests
- **Label** personal data by purpose, defining allowed use cases only
- **Control** deletion or de-identification after retention:
 - **Include** backups and data processors

This impacts your data processor selection and contracting processes!

Key Issues: Divide and Conquer the GDPR in Three Areas

How to Attack the GDPR:

Identify processes impacted



Control:

- Identify and document processing purpose
- Document data processed
- Implement conducting PIA
- Train all key staff

Assemble a team



Communicate:

- Appoint a DPO
- Review privacy policies
- Prepare breach notification

Appoint mandated owners

Document risks



Subjects:

- Prepare for subject rights
- Determine request handling procedures
- Apply processor agreements

Actionable Recommendations — Throttle, Brakes, Balance

- ✓ **Appoint and mandate** business process owners.
- ✓ **Appoint** the data protection officer.
- ✓ **Define and document** processing purposes.
- ✓ **Motivate** personal data processed.
- ✓ **Define and implement** retention periods.
- ✓ **Purge** excess data accordingly.
- ✓ **Prepare** for data subject's rights.
- ✓ **Prepare** for a data breach.
- ✓ **Include** all necessary obligations in agreements with your processors.
- ✓ **Maintain** compliance: Control new initiatives in the meantime.
- ✓ **Audit** annually to identify remaining compliance gaps.

Action Plan After Today

Monday Morning/Next Week:

- *Diagnose* prioritization of actions and *obtain* approval from business stakeholders.
- *Assemble* your team, *involve* the data protection officer.

Next 90 Days:

- *Launch* a PIA to identify and connect purposes, data and measures.
- *Obtain* valid, purposeful consent where you can.
- *Deidentify* the data you do not need in identifiable form.

ASAP Afterward:

- *Ensure* compliance today and *control* new initiatives in the meantime.
- *Investigate* new technology relevance and *prepare* to adopt on time.
- *Fire drill* where you can!

Master the Bike Before Improving Lap Times.

Recommended Gartner Research

- ▶ [Maverick* Research: The Disappearing Customer](#)
Jenny Sussin, Ed Thompson and Others (G00332363)
- ▶ [GDPR Clarity: 19 Frequently Asked Questions Answered](#)
Bart Willemsen (G00333107)
- ▶ [Hype Cycle for Privacy, 2017](#)
Bart Willemsen (G00314626)
- ▶ [Toolkit: Privacy Impact Assessment Quick Scan](#)
Bart Willemsen (G00320185)
- ▶ [The Four Do's and Don'ts of Implementing Your Privacy Program](#)
Bart Willemsen and Prateek Bhajanka (G00319945)
- ▶ [The Impacts of the General Data Protection Regulation on MDM](#)
Simon James Walker and Bart Willemsen (G00319939)

For information, please contact your Gartner representative.