Diligent

Brace for Impact:

Why the GDPR Should Remain at the Top of Directors' Agendas

The ICSA Annual Conference 2017
Stronger Boards, Better Governance
ExCel, London, 4 July, 2017, 11:30 AM

Our Panelists

- Dottie Schindlinger
  VP & Governance Technology Evangelist
  Diligent Corporation
- Stephen Page
  Head of Legal & Compliance
  Blueprint OneWorld
- Victor Shadare
  Sr. Security Engineer
  Diligent Corporation

About the GDPR - General Data Protection Regulation

- **Fines for breach**
  - ✓ Up to 4% of annual worldwide turnover (or €20 million – whichever is greater)
  - ✓ Applies to all data controllers & processors in the EU, or that target EU citizens
- **DPO** – Data Protection Officer – appointment required
- **Accountability** – companies required to establish/prove accountability for data protection
  - ✓ Regular reviews & assessments of data processing procedures
  - ✓ Minimising data processing & retention
  - ✓ Strong safeguards to protect privacy
  - ✓ All processes must be documented, and approved by directors/senior officers
- **Privacy impact assessments** required for large-scale data processing projects, and privacy should be the design of all data processing projects
- **Explicit, signed, freely given consent** by customers to collect, process, store, and access data
- **New rights for consumers** – they now rights to:
  - ✓ Review data being collected/processed
  - ✓ Revoke consent, and be “forgotten”
  - ✓ Data portability
  - ✓ Object to data profiling
- **Mandatory breach notification** of 72 hours
- **Registration** – data processors must be registered entities

“Evolutionary or Revolutionary?”

- **Your answer may show where your are on the “Path to GDPR Enlightenment” (or GDPR Compliance…)**

Why Should the GDPR Remain on the Board's Agenda?

New Definition of Consent under GDPR:

*"Any freely given specific informed and **unambiguous indication** of the data subject's wishes by which he or she by **a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her."*

- New requirements for "consent" could have a dramatic impact on business.
- Many businesses may find the basis on which they are using clients' data cannot be sustained under GDPR.
- Consents collected prior to GDPR may no longer be acceptable.

Best Practices – Some “Do’s”

DO:

- **Check existing consents:**
  - ✓ “Refresh” if necessary, but beware of dangers!
  - ✓ Review at appropriate intervals
- **Ensure consent is the most appropriate “lawful basis” for processing:**
  - ✓ Contract (best of all?)
  - ✓ Compliance with legal obligation under EU law
  - ✓ Vital interests
  - ✓ Legitimate interests (including commercial benefits)
  - ✓ Public task (Public authorities only)
- **Be specific clear and concise:**
  - ✓ Granular “unbundled” consent required
- **Keep evidence and document processes:**
  - ✓ Maintain a record of when and how consent was obtained
  - ✓ Spreadsheet details not sufficient: need to be specific
  - ✓ Include name of the organisation seeking consent
  - ✓ Make sure processes are properly documented
  - ✓ Compliance must be demonstrated

And some “don’ts”…

- **Do NOT assume consent is forever** – it’s not!
- **Do NOT use “pre-tick” boxes** or consent by default – active “opt-ins” are required
- **DO NOT EXPOSE YOUR ORGANISATION TO ADMINISTRATIVE FINES:**
  - ✓ Up to €20 million or 4% of the total worldwide annual turnover whichever is higher for “basic principles for processing, including conditions for consent”
  - ✓ (€10 million or 2% for inadequate record keeping)

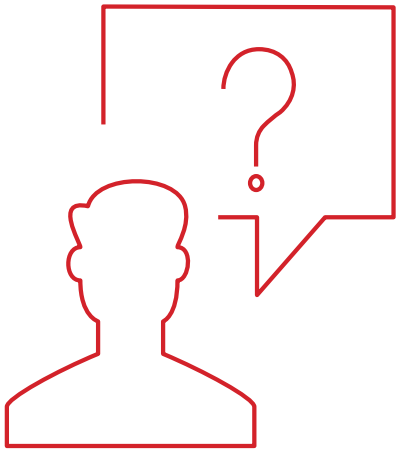
The Good with the Bad

But think of the positives…

- GDPR provides a licence for business to use data – make this a virtue
- Business relationships can be strengthened and flourish on the basis of mutual trust
- Embrace GDPR – it's not going to go away even post-Brexit!

Diligent

Are Directors ready for the new cyber landscape of GDPR?



Survey of Director Communication Practices & Cyber-Readiness

Respondents were directors of NYSE companies (n=381)
Survey focused on ▶

- **Board Communication Methods**
  how sensitive board information is currently managed
- **Effectiveness of Board Communications**
  how effective are board communications
- **Awareness**
  how aware are directors of the risks inherent in board communications
- **Controls**
  what systems do boards currently use to mitigate & manage communications risk

Diligent

What methods do directors use to communicate?

92%

use personal email to communicate with fellow directors & management

Diligent

How often do directors download board books or company documents onto personal computer or devices?

54%

Half the time

Diligent

Who sanctions directors' communication methods?

8%

IT, IS or Data Security Team

15%

Legal or Corporate Secretary

16%

Audit or Risk Committee

27%

Board Chair or Lead Director

5%

"No one"

Diligent

Has the board conducted a security audit of its communications practices?

68%

"Don't Know" or "Management sees to this aspect"

Diligent

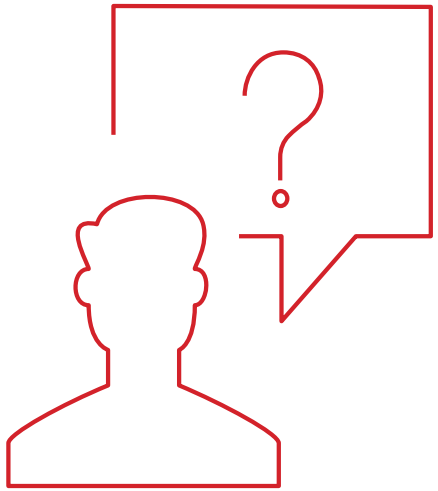
Are directors required to participate in cybersecurity training?

62%

Said “No”

Diligent

Learn more…



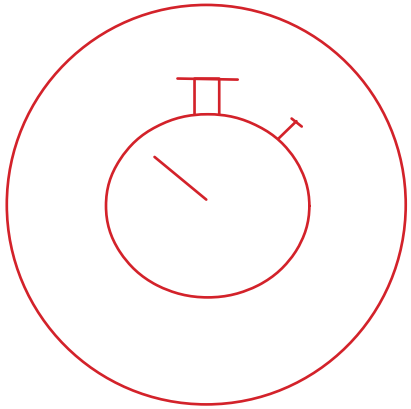
Get the full report

learn.diligent.com/ThePriceofConvenience

Diligent

Diligent

It’s Time for a New Strategic Partnership – The Board & IT



Considerations for Directors

As an organisation's data becomes **more accessible via mobile devices and the cloud**, it is essential for the organisation have **strategic measures that ensure data is properly protected.**

- Security oversight of information repositories & access to those repositories
- Good governance
  - ✓ Identification of information held and the specific locations of such information
  - ✓ Who has access to the information and what the individual can do with the information (copy, attach to email, print etc.)
  - ✓ CTO/CISO providing access to the board
  - ✓ Appointment of a DPO (with direct accountability to the board)
  - ✓ Good data handling training program specifically for directors

Info Security Team & Directors – Strategic Partners

To ensure GDPR compliance, the board cannot afford to assume “IT will handle this”

- Reduce the false reliance on “software” to handle GDPR compliance
- Increase directors’ understanding of the company’s data security posture, programs, testing, and auditing
- Ensure directors are kept informed as incidents come to light – not only after a breach has been remediated
- Cyber risk insurance isn’t enough

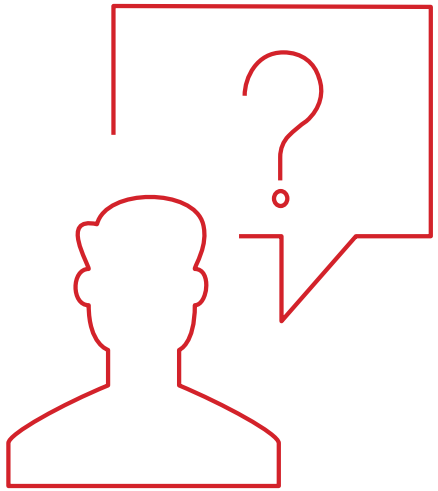
Encourage Directors to Use Encrypted Tech

The time has never been better to digitise the governance process.

- Digital board papers can be encrypted, controlled, archived, tracked, and wiped from lost/stolen mobile devices
- Secure messaging apps can help directors communicate through closed-loop, encrypted channels – rather than through unsecured personal email accounts

- Taking board information online means directors have a verifiable record demonstrating their accountability – dates/times of reports can be cross-referenced with director login data

Questions & Discussion



What's on Your Mind?

Diligent