

Compliance stakes, GDPR and beyond...



Chairman:
Luciano Guglielmi
Gruppo Arnoldo
Mondadori Editore



Chairman:
Federico Cilloccu
Gruppo Arnoldo
Mondadori Editore



Facilitator:
Andrea D'Agostino
Gruppo Arnoldo
Mondadori Editore

What we have found!

The key conclusions from the session:

- GDPR may be an opportunity for IT and for company to better understand and manage personal data
- CEO has the accountability to get the company GDPR compliant, but it is an interdepartmental responsibility
- Culture change on privacy awareness is one key point for a successful GDPR introduction

What we have explored

Among these conclusions, we have developed one of these in greater detail below:

Data management divided in 4 phase (Discovering - when, where, why data are handled, Fix and security)

For internal data processing:

- DTM/IDTA (data transfer management, intra company data transfer agreement) to collect data or records of process approach

For external data processing:

- Contract review via procurement on requirements for GDPR compliance. Reassess contracts with 3rd party on a regular basis (yearly) to stay compliant

What we have left open...

Some questions still remain to be addressed:

- We left open Data Portability and minor GDPR requirements that we have decided to approach in an easy way in spite of the main important principals provided by GDPR
- All process related GDPR topics (e.g. data retention, data subject requests)

Convergences

What points do we share in common:

We agree that by 25 of May 2018 all companies will not be 100% compliant to GDPR considering that there is too many open points to be implemented by the national legislator
DPO and awareness of privacy are preparatory to all implementations of GDPR
DPO is a legal professional

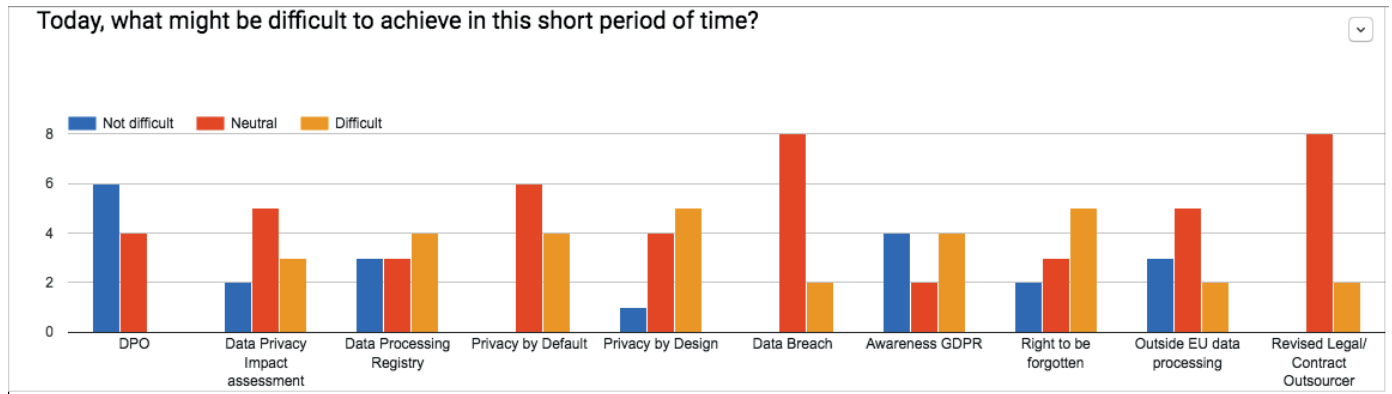
Differences

What points do we agree to disagree:

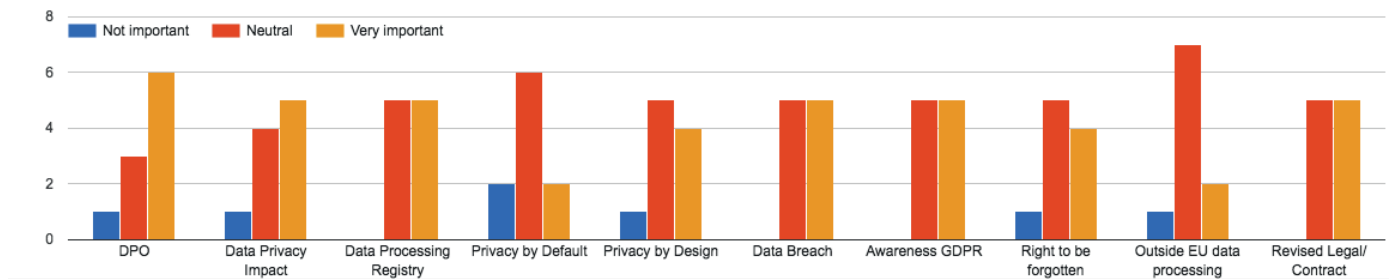
Who has the budget, the DPO or the the CIO?
GDPR is a great lever to foster security on privacy data – from an IT perspective: it is to avoid any data breach
DPO will be just one person or a specific corporate unit governed by one person

A picture is worth a thousand words

An illustration that sums up our results:



What are main conditions you think must be achieved until May, 28 2018 abling your company to be compliant with GDPR?



- IT Level
- BUSINESS Level
- LEGAL & COMPLIANCE Level
- HR Level
- SUPPLIER level

ALL COUNTRIES ARE WAITING FOR "LOOSES" ADDITION GOING FROM NATIONAL PRIVACY & LEGISLATIVE AUTHORITY

IT Dpt

Legal Dpt

1 2 3 4 5

ONE OFF COSTS

RECURRING COSTS

DPO ORGANIZATION

YES NO

(LEGAL)

K-F-P
Free Data Conference Service