

May 26, 2021

Flexibility by Design:

Adapting Your Privacy Program to Shifting Compliance Challenges

Speakers



Maureen Dry-Wasson

VP-Group GC and Global
Privacy Officer
Allegis Group



Constantine Karbaliotis

Counsel
nNovation LLP



Gordon Wade

Data Protection Officer &
Group Legal Counsel
Hostelworld Group



Mark Smith

Principal Legal Analyst –
Privacy & Data Security
Bloomberg Law

AGENDA

- Review & Assess
 - Building a Flexible Team
 - Evaluating Frameworks
 - Using External Resources
 - Implementation & Messaging
 - Forecasting & Preparing for Change
-
- ❖ Practical Takeaways
 - ❖ Roundtable Discussion
 - ❖ Questions Encouraged!



Review & Assess

Review & Assess

- **Know your company / know the culture**
 - Who are the decision makers?
 - Who are the agents of change?
- **Identify stakeholders**
 - Internal (C-Suite, Finance, Legal, IT, Support)
 - External (customers, regulators)
 - Know how to engage (and reengage)
- **Assess Expectations**
 - Realistic compliance goal (perfection is not realistic)
 - Most stringent regime?
- **Budgetary considerations**



Building a Flexible Team

Building a Flexible Team

- what are the key roles?
- lawyers v. non-lawyers
- backgrounds and talents
- recruiting champions/liaisons
- making converts
- how to stay current
- make investments in team
- partnerships with infosec, IT



Evaluating Frameworks

Evaluating Frameworks

- There are many good frameworks, that address many of the same things
- Key is the ability to map to regulations that govern you - it's easier to comply with a framework than multiple laws
- Considerations in selecting a framework:
 - Whom do you need to impress?
 - What does InfoSec use - NIST, ISO, GAPP?
 - Are/will you be seeking SOC II?
 - What does your client/regulator audience expect? - speak their language
 - Evidence-based



Flexibility by Design

Allegis Group's Data Protection Readiness Program

1 Understanding Our Data – Data Mapping and Justifications for Processing

- Completion of data mapping exercises
- Completion of our Article 30 records of processing activities under GDPR
- Understanding where we “sell” personal data under CCPA

3



Contracts – Customers and Suppliers

- Implementing DPR compliant provisions in our contracts with our customers and suppliers
- Conducting due diligence on our suppliers through questionnaires and, where appropriate, on-site or other forms of audit

4



Training and Awareness and Appointment of Data Protection Officer

- Appointment of Lillian Pang as Data Protection Officer under GDPR
- Online and in-person trainings across the business to promote privacy awareness and teach key privacy principles

2



Data Breach Reporting

- Ensuring our privacy and security incident response process is prepared to respond within various DPR deadlines

5



Data Subject Rights and Consent/Preference Management

- Implementing a repeatable, scalable process and set of procedures for handling data subject rights requests
- Implementing and adhering to consents and preferences expressed by data subjects



Flexibility by Design

Allegis Group's Data Protection Readiness Program

6



Data Transfers

- Ensuring we are maintaining viable means for transferring personal data, including maintaining a Global Intra-Group Data Transfer Agreement, based on the model clauses and Article 28 of GDPR, and executing model clauses where needed with customers and suppliers for the EU and Switzerland

8



Information Security

- Partnering closely with our Information Security team to implement appropriate technical and organizational measures to protect personal data, including looking for opportunities to enhance the use of anonymization, pseudonymization and encryption

9



Privacy in Day-to-Day Operations/ Privacy by Design and DPIA

- Undertaking Data Privacy Impact Assessments (DPIAs) where appropriate across the business
- Partnering with our Privacy and Protection team within IS for Privacy by Design
- Educating areas of the business (e.g., HR, Marketing, Procurement) on the meaning of privacy for their function in day-to-day operations

7



Data Minimization

- Ensuring that Allegis Group collects and keeps only data that is necessary for its legitimate business interests



10



Privacy Notices

- Updating and distributing all privacy notices to remain in compliance with DPR

Using Resources

Using Resources

- Excel and Outlook aren't scalable
- Many firms undertake their own development, but this is software development; consideration must be taken of what maintaining tools will cost in terms of resources
- Key considerations for software selection:
 - Point solution? Don't just pick a PIA tool, consider vendor management, consent, DSAR...
 - Integrations are key - can the tool pick up data from other sources? Can it feed other tools (GRCs or incident management)?
- Outside Counsel



Implementation & Messaging

Implementation & Messaging

- HR
- Sales/Marketing
- Product
- Consumers

Annual reviews and cross-checks

Privacy is a team sport; involvement and acceptance of policies is essential as structures imposed 'from the top' rarely have a chance for success



Forecast

Flexibility by Design

Forecasting & Preparing for Change



Privacy Shield
Framework



Questions?





Maureen Dry-Wasson

VP-Group GC and Global
Privacy Officer

Allegis Group

mdry@allegisgroup.com



Constantine Karbaliotis

Counsel

nNovation LLP

ckarbaliotis@nnovation.com



Gordon Wade

Data Protection Officer &
Group Legal Counsel

Hostelworld Group

Gordon.Wade@hostelworld.com



Mark Smith

Principal Legal Analyst –
Privacy & Data Security

Bloomberg Law

mark.smith@bloomberglaw.com