

Blackboard

Blackboard – Implementation of the GDPR

ALT webinar

Stephan Geering, Global Privacy Officer

April 2018



Introduction / Bio

Global Privacy Officer

- Global responsibility for compliance with data privacy and security laws
- Leads Global Data Privacy / GDPR implementation programme
- Reporting to Chief Legal Officer; member of Blackboard's Legal team
- Based in London
- CIPP/E certified



Stephan Geering

My Background

- Lawyer / Deputy Data Protection Commissioner at a Swiss cantonal Data Protection Authority (2002-2008)
- LLM at University College London (2008-2009)
- Associate Director, Group Privacy at Barclays (2010-2012)
- EMEA Regional Head of Data Privacy Operations at Citigroup (2012-2014)
- EMEA and APAC Chief Privacy Officer at Citigroup (2014-2017)

Content



- GDPR – Requirements and myths
- The importance of data privacy
- GDPR – Our programme
- GDPR – How our programme helps our clients
- Implementation tips
- How we translated GDPR requirements into practice
- Questions
- Appendix – Helpful resources



GDPR – Requirements and myths

EU General Data Protection Regulation (GDPR) - Background

- Most **ambitious and comprehensive** changes to data protection rules around the world in the last 20 years - Compliance date: 25 May 2018
- **Aim:** Harmonisation, enhanced right of individuals, stronger enforcement
- **Main target:** US internet services such as Google and Facebook
- **Key changes:**
 - Fines of up to 4% of global turnover
 - Extended territorial scope
 - Mandatory breach notification
 - Enhanced right of individuals: Right to erasure (“right to be forgotten”), right to be not subject to a measure based on automated decision-making
 - Principle of accountability: documentation of compliance
- **Some concepts stay the same:**
 - Wide definition of “personal data”
 - Security measures need to be appropriate (to the risk)
 - Existing data privacy principles remain



Source: IMDB

GDPR “myths”

Consent required

Myth: Consent is required for all processing of personal data

Fact:

- Consent is just one of several legal bases (e.g. performance of contract, legitimate interest)
- Bar for consent has become very high (requires genuine choice)
- Often other legal bases will be more suitable

72h breach notification period

Myth: 72 hours start from the moment a vendor becomes aware of a breach

Fact:

- Vendor (data processor) needs to notify data controller “without undue delay”
- 72 hours period only starts once the data processor has notified the controller
- Note: 72 hours “where feasible”

GDPR “myths” (continued)

No data transfers outside the EU

Myth: Data transfers outside the EU/EEA are not allowed or only with the client’s consent for each data transfer

Fact:

- Allowed as Blackboard has EU approved data transfer mechanisms (e.g. Privacy Shield or EU-approved model clauses) in place.
- General instruction by client sufficient

Right to be forgotten

Myth: Right to erasure requires organisations to delete all data about an individual

Fact:

- Right to erasure is not an absolute “right to be forgotten”
- Personal information that is still legitimately required does not need to be deleted

The Importance of data privacy

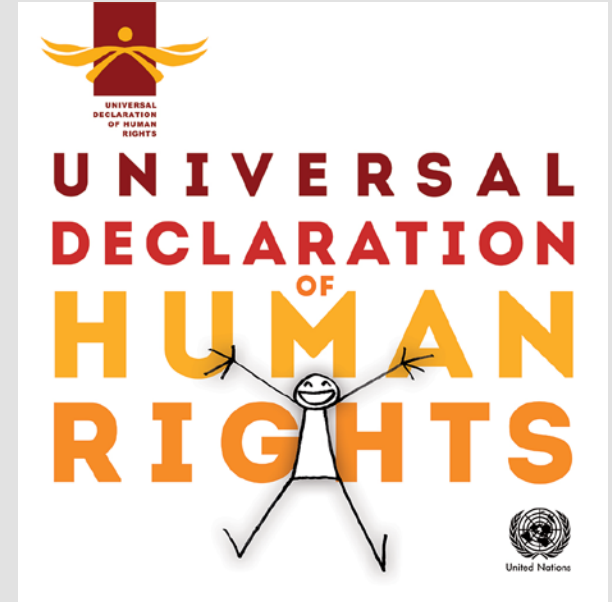
Why is data privacy so important?

How good data privacy practices add value (the positive case)

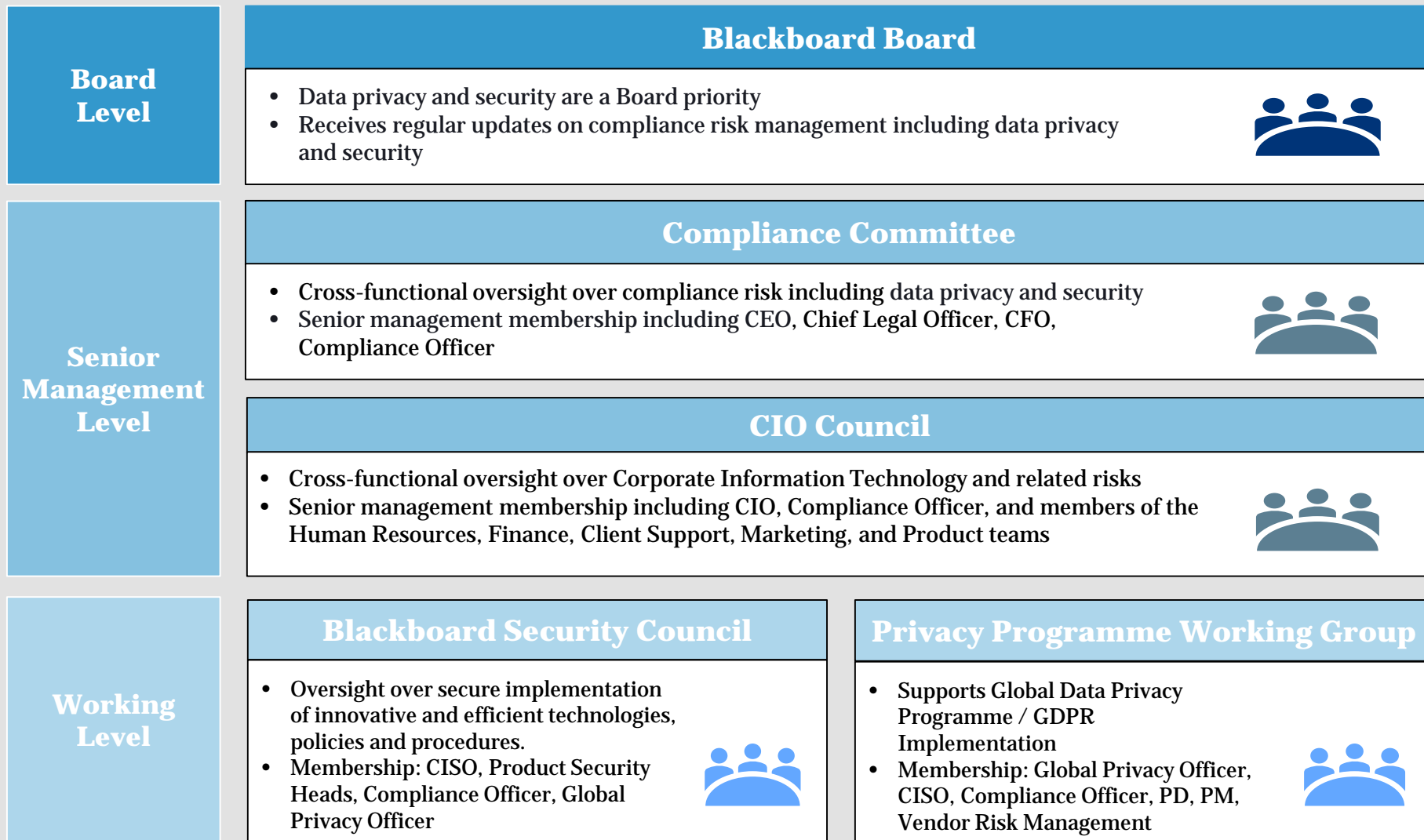
- Data privacy is a human right
- Data privacy is a competitive advantage
- Good data privacy practices mean better data management
- Builds trust
- Students (and staff) more likely to share data and use new tools, which helps Blackboard help them

When things go wrong ... (the negative case)

- Reputational damage
- Losing trust of students
- Individual claims
- Regulatory enforcement



Our data privacy and security governance



GDPR – Our programme

Our GDPR approach and plan

Approach

- Builds on Blackboard's existing privacy experience and compliance mechanisms
- Led by Global Privacy Officer and supported by a dedicated project manager and "GDPR Leads" in each functional area
- The renowned law firm Bristows LLP, among several others, has been engaged to support the project
- The project is overseen by Blackboard's Compliance Committee, which includes the company's CEO, Chief Legal Officer, and other senior officers

Project Initiation

- Senior management briefing and buy-in
- Hiring of a Global Privacy Officer with GDPR responsibility
- Development of project plan and project governance
- Initial information gathering and assessment of current compliance

Phase 1 - Information gathering (workshops)

- Structured workshops with key stakeholders from Blackboard's functional areas to obtain detailed information about data processing practices
- Output will be used to develop the solutions and implementation plans

Phase 2 - Development of solutions

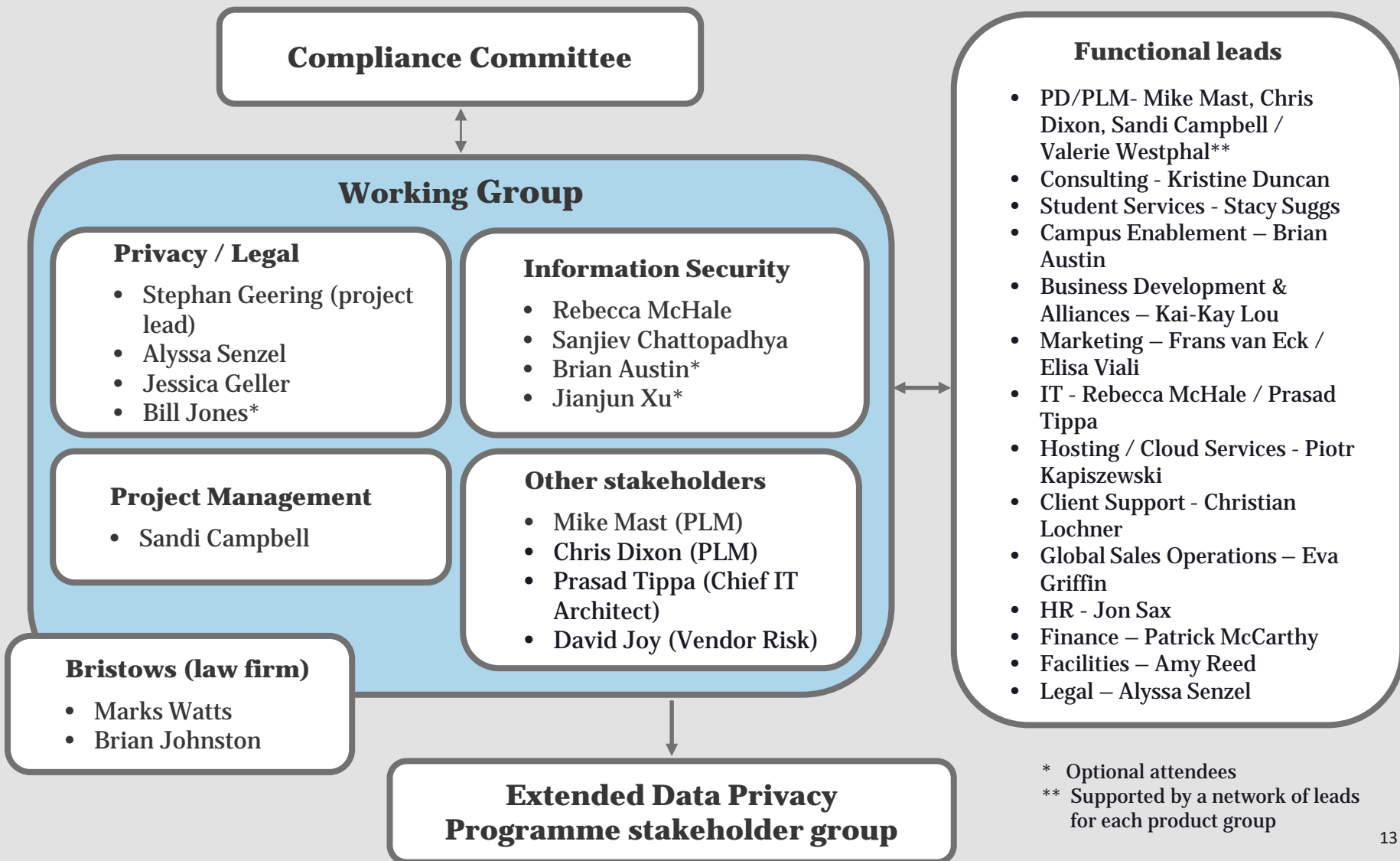
- Enhanced internal privacy documentation (policy and detailed operational standards - e.g. requirements for processing of customer/student data)
- Implementation plans for the functional areas and for centrally required efforts

Phase 3 - Implementation workstreams

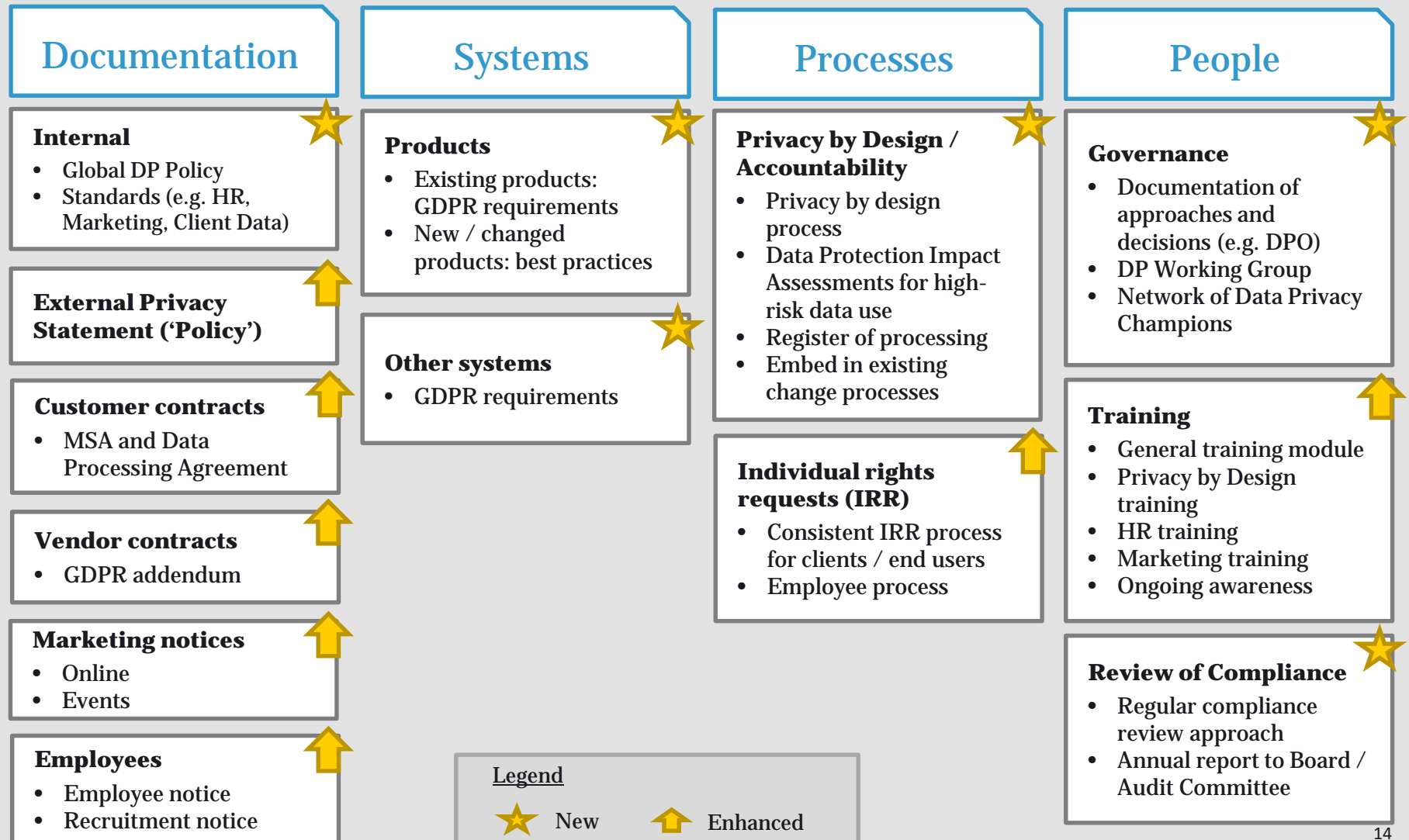
Implement privacy documentation and execute implementation plans :


1. Execution of implementation plans for the functional areas
2. Review and update of public-facing policies, notices and consents
3. Enhancing governance (training, Privacy Impact Assessments, etc.)
4. Review and updates of vendor contracts (where necessary)
5. IT systems changes (where necessary)
6. Establishing data processing register

Data Privacy / GDPR Programme - Governance



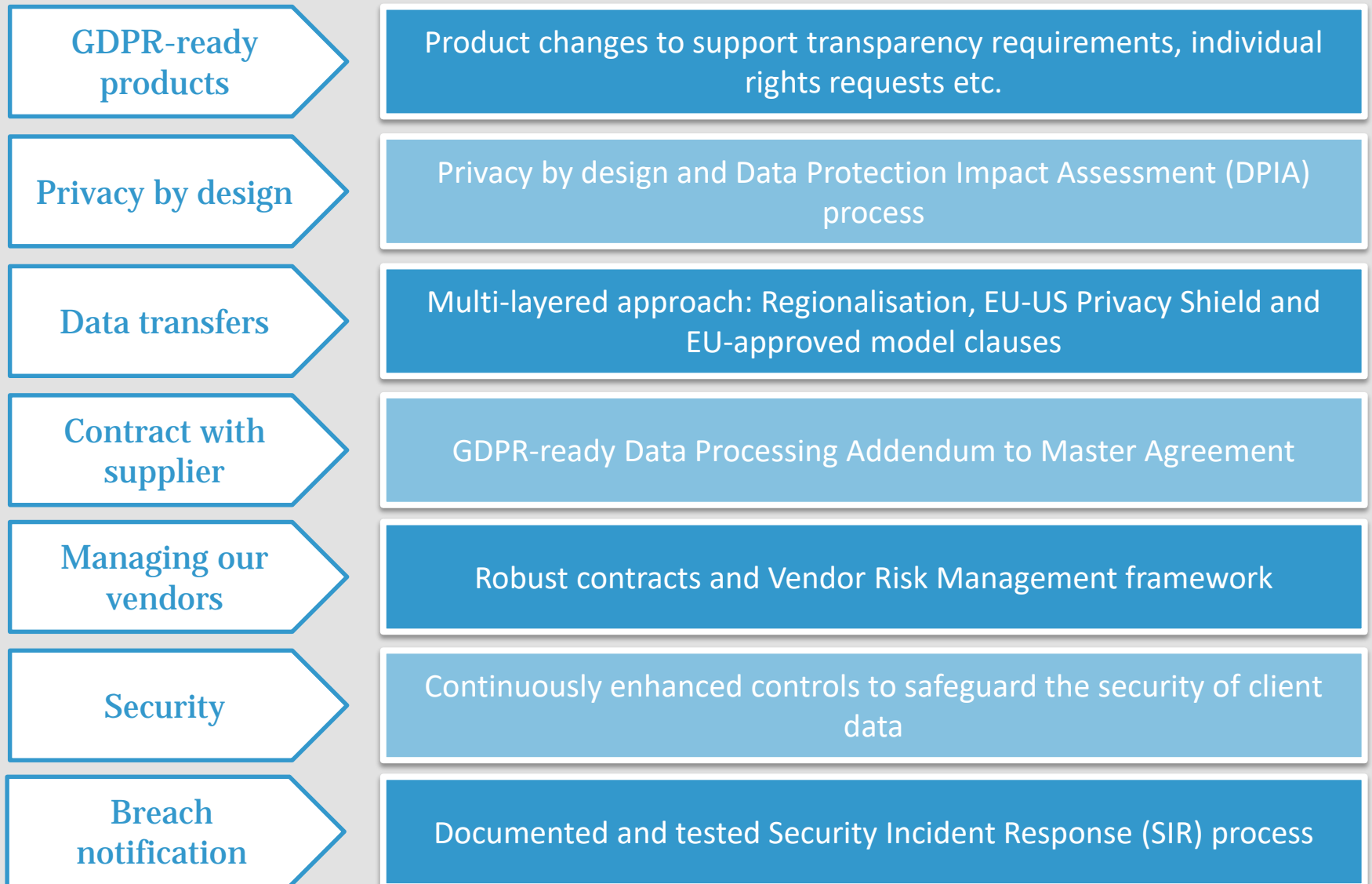
Data Privacy / GDPR Programme – Envisaged end state





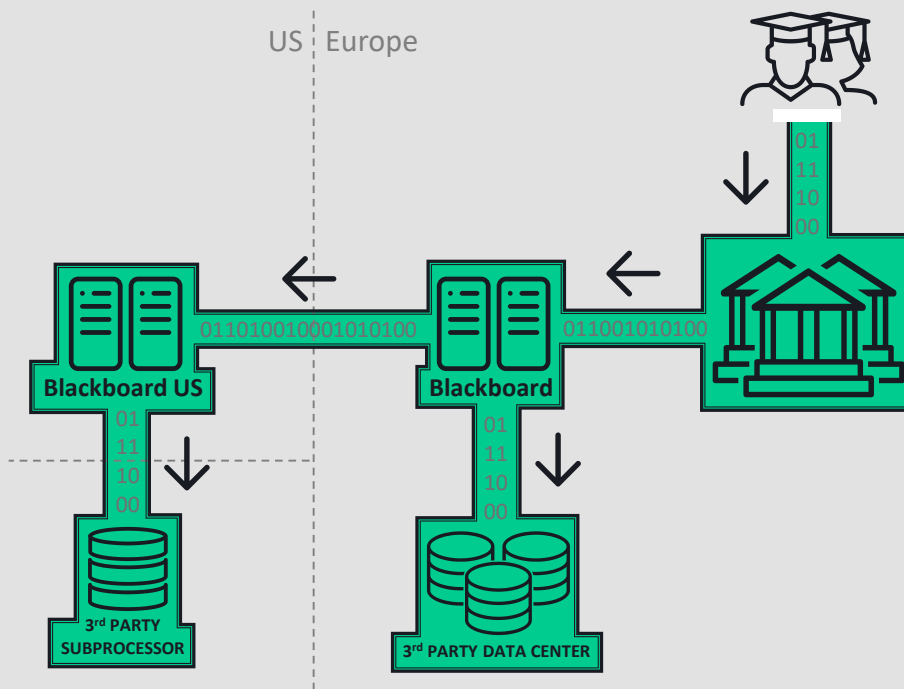
GDPR – How our programme helps our clients

GDPR –How Blackboard can help you



Data transfers: Multi-layered approach

BLACKBOARD'S APPROACH: *Multi-layered and Redundant*, meeting the requirements via multiple avenues to ensure the proper safeguards are in place for your transferred data.



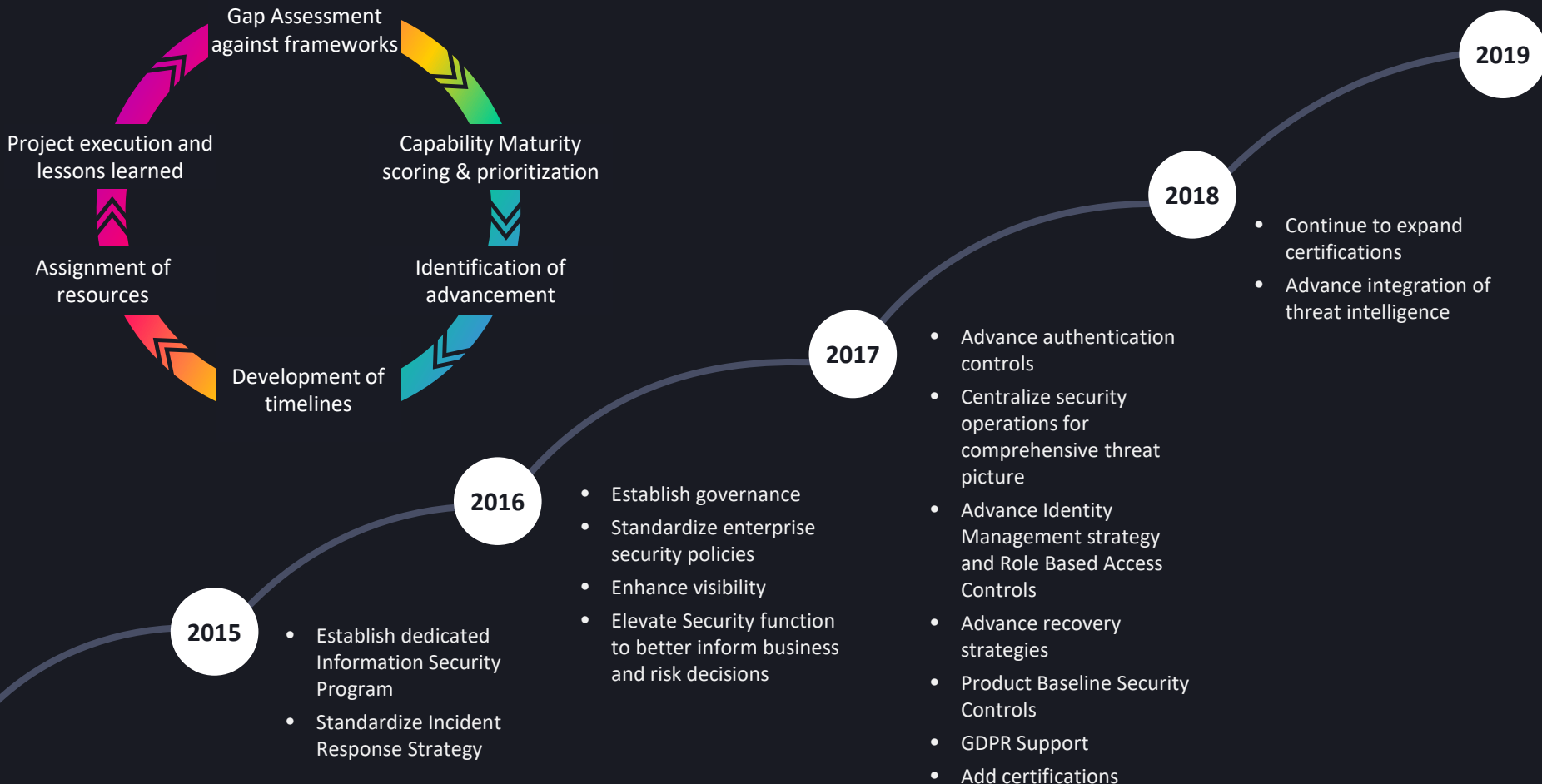
Regional hosting: Many EU clients prefer data to be kept inside the EU even if not required by the GDPR. We therefore have a regional hosting strategy.

Privacy Shield: Blackboard is EU-US Privacy Shield certified ([link](#)) which allows us to lawfully transfer personal information to the US.

Model clauses: We also use EU-approved “model clause” agreements that allow us to compliantly transfer personal information outside the EEA (“Customer Data Transfer Agreement”).

Vendors: Robust contracts are in place with vendors (e.g., IBM, Amazon Web Services) to ensure that data transfer requirements are passed on to our vendors.

Adopting frameworks: Security maturity assessments & roadmaps



Implementation tips

Implementation approach and project

1. Check if the GDPR applies to your organisation

- If your organisation is established in the EU then the GDPR applies
- But the GDPR may also apply to organisations outside the EU

2. Establish a GDPR project

- Design and implement a dedicated GDPR project
- Ideally you will have project management support and nominated contacts who can support you in every department

3. Nominate an experienced GDPR lead to manage the project

- Should be an experienced data privacy lead
- Needs to have sufficient time and resources as well as access to external support (e.g. law firm)
- If your organisation is a public authority established in the EU, you will also need to appoint a Data Protection Officer

Implementation approach and project (continued)

4. Ensure senior management buy-in and oversight

- Required for successful implementation of GDPR project
- Provides (escalation) support, direction and oversight

5. Review your use of personal information and conduct gap analysis

- Understanding where and how personal information is used
- Determine where GDPR enhancements are required

6. Develop action plans to close gaps

- Requires translating the often high-level requirements of the GDPR into specific and practicable actions for all the various processes and systems
- See slides 9ff.

Tips for the implementation phase

Approach:

- Make teams/departments responsible for their actions
- 25 May is just the beginning!

A few key points:

- Privacy Statement: clear and plain language ... but also very detailed – layered approach?
- Training and awareness
- Data Protection Officer – can be one single DPO for several public authorities (Art. 29 Working Party guidance)
- Marketing – different rules (ePrivacy Directive) but increased focus on heightened standards for consent
- Individual rights – processes and managing expectations
- Legacy issues (records management? security?) – regulatory leniency unlikely to apply
- Stay abreast of legal / regulatory developments (Art. 29 Working Party guidance, Member States implementing laws)

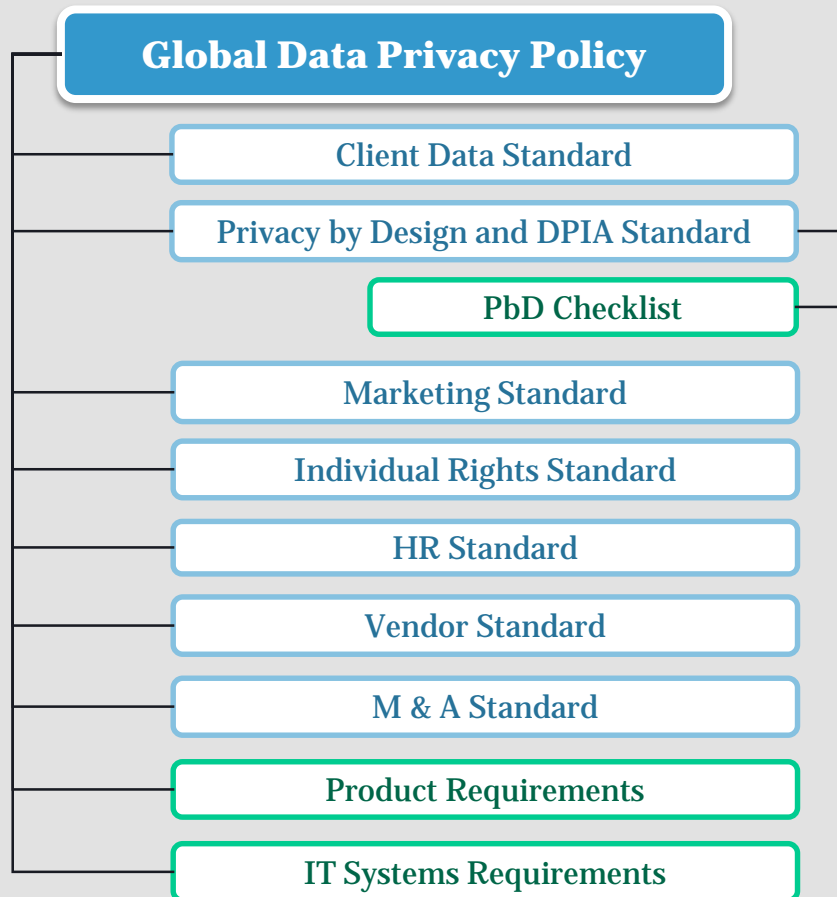


How we translated GDPR requirements into practice

Internal Global Data Privacy Policy and Standards

GDPR requirement (Art. 24(2))

- Implement data protection policies (where proportionate in relation to processing activities)



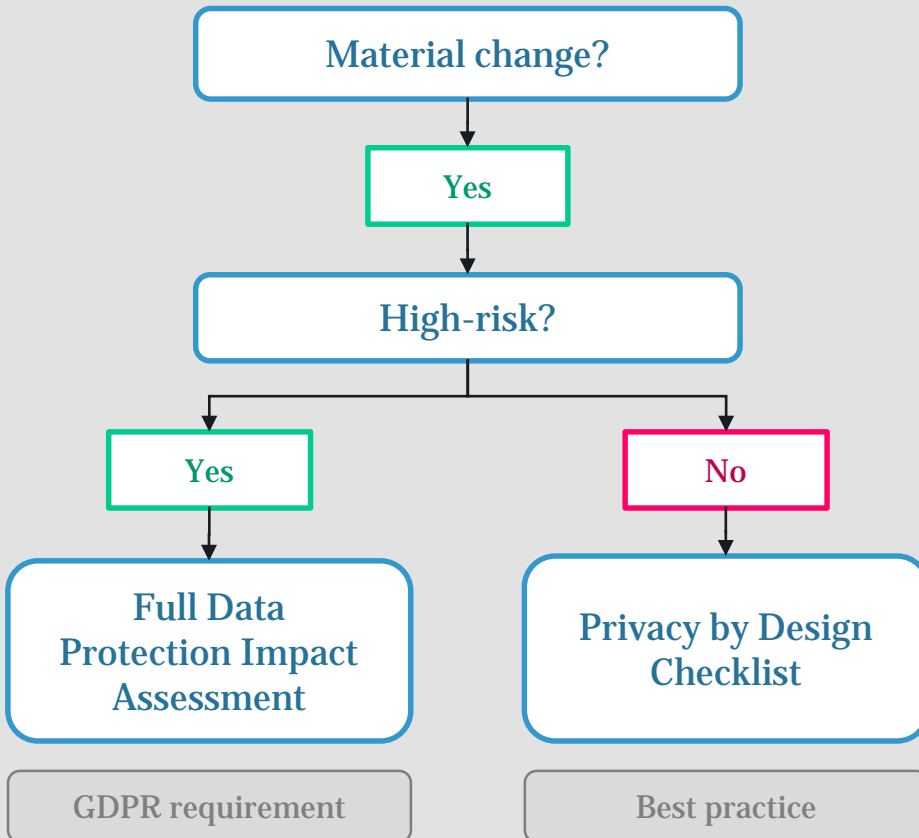
Approach

- Internal Global Data Privacy Policy describes the 10 data privacy principles for Blackboard and the related governance (e.g. roles & responsibilities)
- Supported by standards for particular data categories and activities
- Policy and standards define the requirements that Blackboard departments and staff need to comply with
- Scope: Global with some EU-specific sections
- Leveraging the following documents:
 - Security Incident Response (SIR) Plan
 - Records Management Policy

Privacy by design and data protection impact assessments (DPIA)

GDPR requirements

- Implement technical and organisational data privacy by design measures (Art. 25(1))
- Conduct data protection impact assessments (DPIA) for high-risk processing (Art. 35)



Approach

- Not a revolution: formalisation and enhanced documentation of existing legal reviews
- Supports the principle of accountability: Document and demonstrate compliance
- Departments need to establish “trigger points” in their change processes
- Every material change in how personal information is used requires completion of a Privacy by design checklist (“mini DPIA” – best practice)
- Checklist will trigger more detailed Data Protection Impact Assessment (DPIA) for high-risk use of personal information (GDPR requirement)
- Tool (WireWheel) to automate review

GDPR-ready products

GDPR requirement (Art. 28(1))

- Only use vendors that provide sufficient guarantees that processing meets GDPR requirements

Security

- Covered by existing information security programme for products

Transparency

- Ability for clients to link to their policies/notices
- Provide information on how personal information is generally being used

Data Minimisation / Deletion

- Review for unnecessary / optional fields
- Review for opportunities to use of pseudonymous or anonymous data
- Ability to delete data when requested by clients (where client / user cannot delete data themselves)

Individual Rights

- Ability to provide access and correct personal information when requested
- Ability to delete personal information when requested

EU Rights

- Ability to deal with data portability requests (right to receive data in machine-readable format in certain circumstances)
- Ability to stop using personal information (right to object / right to restriction in certain circumstances)

Approach

- Scope: Global requirements with some EU-specific additions
- Initial version developed with external counsel
- Refined into actionable general product requirements with Product Management and Product Development
- Translated into product specific actions (product implementation plans)
- Requirements are supported by detailed guidance

Data processing agreements (DPA)

GDPR requirements (Art. 28(3) plus Art. 28(2) and (4))

- Agreement needs to be in place with vendors (“data processor”)
- Detailed list of required points to be included in agreement with data processor

Blackboard’s standard DPA includes all the required points:

- ✓ Use personal data only as instructed
- ✓ Vendor staff must sign confidentiality agreements
- ✓ Vendor must have appropriate security measures in place
- ✓ Only engage further vendors (sub-processors) ...
 - As authorised by data controller (can be a general authorisation)
 - That are contractually required to follow the same data protection obligations
- ✓ Assist controller with responding to individual rights requests
- ✓ Assist controller with security measures, breach notification and data protection impact assessments
- ✓ Returns or deletes data at end of contract
- ✓ Provide information that is necessary for the data controller to demonstrate compliance
- ✓ Immediately inform data controller if any instructions from data controller are in breach of GDPR

Approach

- Proactive approach to help clients: Our DPA applies as the minimum standard for agreements without GDPR provisions
- More favourable provisions in old DPAs are also applicable (if not conflicting)
- [More information](#)

Managing vendors: contracts are not enough

GDPR requirements (Art. 28)

- Agreement with specified content (see previous slide)
- Only use vendors that provide sufficient guarantees that processing meets GDPR requirements
- For data processors: controller authorisation and “down-stream” requirements (Art. 28(2) and (4))

Blackboard’s key vendor controls:

- Robust contracts with partners and third parties which impose materially equivalent provisions that we have in place with our clients through a Privacy and GDPR Addendum developed with external counsel (where applicable)
- “Model clause” agreements and/or GDPR and Privacy Shield Addendum to enable lawful data transfers to our vendors
- Documented Vendor Risk Management policy and framework
- New vendors with access to personal information need to complete a Vendor Security Assessment Questionnaire with data privacy compliance questions
- Vendors with access to Blackboard-managed systems are required to follow Blackboard-internal access control and identity and authorisation policies, to include account reviews as appropriate
- Vendors need to access Blackboard resources through approved mechanisms (e.g. VPN)
- Vendors have restricted access controls on traffic, users, and assets

Why and how we use vendors

- Blackboard uses vendors (e.g. IBM, Amazon Web Services) to help us provide our products and services to our clients
- Where this requires access to our clients’ personal information, Blackboard is responsible for the data privacy practices of the vendors

Mandatory breach notification

GDPR requirements (Art. 28)

- Data controllers (clients): Notify personal data breaches to the competent data protection authority within 72 hours (where feasible) and (in some cases) to the affected individuals without undue delay (Art. 33(1))
- Data processors (vendors): Notify clients without undue delay (i.e. “promptly”) (Art. 33(2))

Blackboard’s established Security Incident Response (SIR) process

- Documented and regularly tested
- Facilitates the swift identification, investigation and remediation in case of an incident
- Allows for prompt notifications to clients
- Relies on the established Security Incident Response team (which includes the Chief Information Security Officer and the Global Privacy Officer)

Questions?

More information:

- [GDPR White Paper](#)
- [Data Privacy and Security group](#) on Blackboard Community
- Blackboard Data Privacy Newsletter (please send me an email to subscribe)

Questions and feedback: stephan.geering@blackboard.com



Appendix - Helpful resources*

Official EU resources

- [GDPR text](#)
- [Article 29 Working Party guidelines](#)
- [EU Commission GDPR website](#)

EU Data Protection Authority material

- The UK Information Commissioner's Office (ICO) has an excellent [GDPR website](#)
- The Irish Data Protection Commissioner (DPC) has a dedicated [GDPR page for organisations](#)
- The French CNIL provides some material [in English](#) including a free Privacy Impact Assessment software

Law firms guides

- [Bird & Bird's guide to the GDPR](#)
- [Bird & Bird's Member State laws tracker](#) (tracking national GDPR variations)
- [Linklaters' GDPR survival guide](#) (PDF)
- [White & Case GDPR handbook](#)

Other organisations

- [JISC](#) UK has helpful resources, events and blog updates on GDPR
- UCISA has published a GDPR [best practice document](#) with practical steps and case studies
- The International Association of Privacy Professionals (IAPP) has a good (free) [weekly newsletter](#) on European data privacy developments
- The IAPP also has a helpful [overview of providers of data privacy tools](#) (PDF)
- Amazon Web Services has a dedicated [GDPR Centre](#)

* The resources linked above are just a small selection of helpful material that is available online. It is not meant to be a comprehensive list.

Blackboard[®]