Blackboard

How Blackboard's GDPR implementation supports our clients

The EU General Data Protection Regulation (GDPR) is a sea change. Blackboard welcomes this change. We care about data privacy and understand that it's a human right. The GDPR strengthens the rights of individuals and will lead to better data privacy practices. This will benefit individuals and organisations as it will increase trust between them.

We are publishing this document to give our clients an overview of the changes and the myths around the GDPR, to explain our implementation approach and to detail how our efforts will support your organisation. We focused on information that we think will be most helpful for you. This white paper is therefore by no means a comprehensive guide to the GDPR.[1]

The GDPR brings significant changes, but at Blackboard we can build on our existing robust data privacy practices (e.g. our EU-US Privacy Shield certification). We see the GDPR as an opportunity to further strengthen our practices. And we will continue to be client-focused and support you with your data privacy compliance.

These materials have been prepared for informational purposes only and are not legal advice. Please seek the advice of your internal or external lawyers for the implementation of the GDPR in your organisation and related legal questions.

CONTENTS

Blackboard is Privacy Shield certified, a proud signatory of the Student Privacy Pledge and a member of the Future of Privacy Forum.

Privacy Shield Certified

STUDENT PRIVACY PLEDGE SIGNATORY

FUTURE OF PRIVACY FORUM

GDPR – WHAT YOU NEED TO KNOW

The GDPR is the new EU data protection legislation that will replace the current EU Data Protection Directive 96/46 (Directive), and the implementing Data Protection Acts in the EU Member States (e.g. the UK Data Protection Act 1998).

The GDPR was enacted in May 2016 with a compliance date of 25 May 2018.

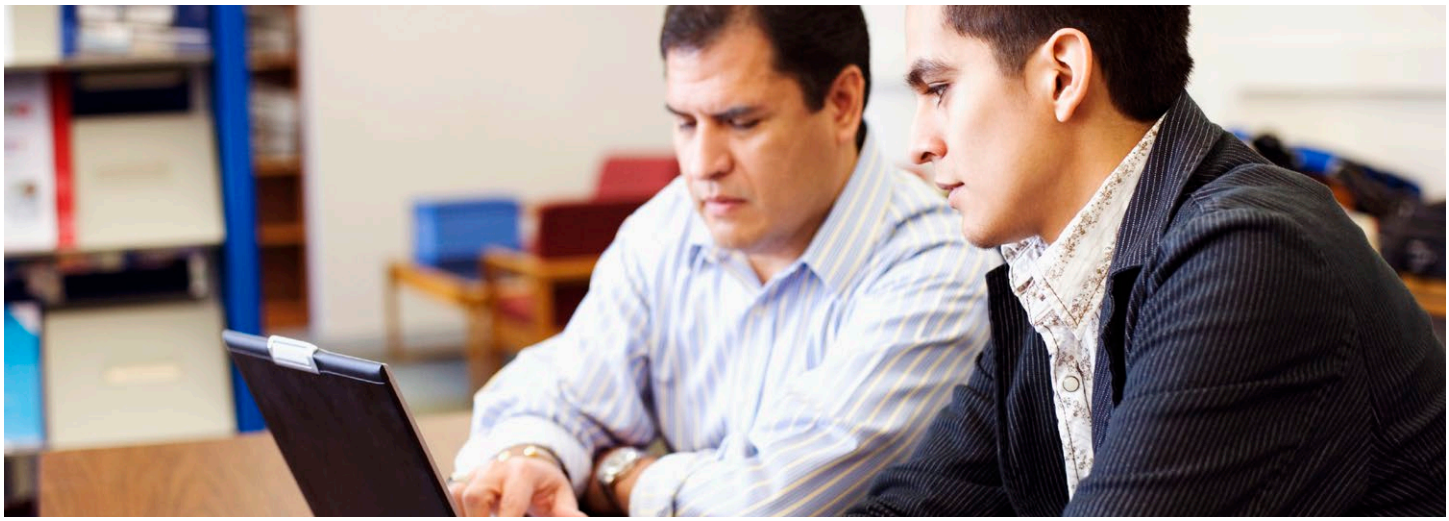
In the sections below, we have provided a very brief (and far from comprehensive) overview of the GDPR requirements. You can find links to more detailed guidance in the "Helpful GDPR resources" section.

Why a new law?

Legislators and regulators in the EU were convinced that the Directive needed updating to address the lack of harmonisation and the societal and technological developments in the 20 years since the Directive. At the top of the list were stronger enforcement powers, wider territorial reach and enhanced rights for individuals.

Many of the new provisions (e.g. extra-territorial effect) are mainly aimed at social media and internet companies outside the EU. EU legislators and regulators felt that the existing Directive did not sufficiently protect the data privacy rights of EU individuals who use such social media and internet services.

Blackboard operates differently from those social media and other internet companies whose model is built on "monetising" user data. We collect and use personal information[2] of our clients at their direction and to provide our products and services to them and their users. We do not collect or use personal information to sell this information or to sell advertising. We understand that personal information is entrusted to us and comes with obligations. We therefore have a shared interest and a shared responsibility with our clients in safeguarding this information.



What is new?

While based on the existing EU data privacy principles and concepts, the GDPR brings significant changes to the data privacy regime in the EU including:

- Increased fining powers of up to 4% of global turnover or EUR 20 Million (whichever is greater)
- Extended territorial scope to organisations outside the EU who provide products and services to EU residents or monitor EU residents
- Mandatory breach notification to supervisory authorities within 72 hours for data controllers[3]
- Stricter requirements regarding consent
- Enhanced rights of the individuals (including the right to erasure and data portability)

But some of the most important changes are the new principles of accountability and privacy by design. These principles require effective data privacy governance and processes as well as more detailed and robust documentation on how an organisation complies with the GDPR requirements.

What stays the same?

Many of the concepts and definitions in the GDPR remain the same or are similar compared to the Directive:

- The definition of "personal data" (or personal information) stays broadly the same but now explicitly includes IP addresses, cookies and device identifiers
- The concepts of "data controller" and "data processor" stays the same (but the GDPR imposes more direct responsibilities on data processors)[4]
- The established principles of processing in the Directive (e.g. lawful & fair processing, purpose limitation, only keeping personal data as long as necessary) are maintained
- The data transfer requirements remain broadly the same: data transfers outside the EU/EEA are permitted as long as an approved data transfer mechanism is used (e.g. EU-US Privacy Shield or "model clauses")[5]

The higher level of fines under the GDPR means that non-compliance with existing principles and requirements such as only keeping personal data as long as necessary or having appropriate security measures in place is likely to carry an increased risk.

What is the impact of Brexit?

The GDPR will be directly applicable in the UK from 25 May 2018 until 'Brexit' at the end of March 2019. But even after Brexit, the GDPR will set the standard for the UK:

- The UK Government has published the UK Data Protection Bill 2017 (currently in the legislative process) which implements the GDPR before and after Brexit[6]
- After Brexit, the GDPR directly applies to UK organisations that offer goods and services to EU residents or monitor them (e.g. UK universities actively recruiting EU students)

Impact on data transfers from and to the UK:

- The EU has clarified that after Brexit the UK will be considered a "third country" which means that is not considered an "adequate" (white-listed) country for data transfers anymore.
- Unless and until the UK is declared adequate by the EU Commission (e.g. as part of a transitional deal), data transfer agreements or other data transfer mechanism need to be put in place for transfers of personal information from the EU to the UK.
- Conversely, the UK needs to determine which countries it deems to be adequate (which would likely include the EU countries and the countries white-listed by the EU). For those countries not deemed adequate, UK-recognised data transfer mechanisms (probably similar to the EU mechanisms) will need to be used for transfers of personal information out of the UK.

Demystifying the GDPR

One aim of the GDPR was to provide more clarity through more detailed prescription. However, there are still many aspects of the GDPR that are open to interpretation. Additionally, the complexity of the GDPR has led to a lack of understanding as well as exaggerated statements. This has created many myths, a few of which we have debunked below:[7]

Myth 1: Consent is required for all processing of personal information

Fact: Consent is just one of several legal bases that allow personal information to be processed (e.g. processing required for the performance of a contract or for the 'legitimate interest' of an organisation). The bar for consent has become very high. For instance, unless the individuals have a genuine free choice and can withdraw their consent at any time without any disadvantage, it will not be considered valid consent. In many data processing scenarios other legal bases will be more suitable.[8]

Myth 2: 72 hours breach notification period applies to the whole supply chain (i.e. from the moment that a (sub)processor is aware of the breach)

Fact: The GDPR requires data processors to notify their data controller "without undue delay" in the case of a personal data breach. Only once the data processor has notified the controller, does the 72 hours notification period for the data controller start. The Article 29 Working Party (WP29), the group of EU data protection authorities has clarified in their final guidelines[9] that that "without undue delay" means "prompt" notification (not "immediate" notification as suggested in a previous draft).

Myth 3: Data transfers outside the EU/EEA are not allowed or only with the client's consent for each data transfer

Fact: The GDPR broadly retains the existing data transfer requirements. As such, data transfers are allowed if an EU approved data transfer mechanism such as the EU-US Privacy Shield or the EU-approved model clauses (data transfer agreements) are in place. Blackboard has both these mechanisms in place to compliantly transfer client personal information.[10] Since Blackboard acts as a data processor, a general instruction for data transfers from the client is required (which is contained in our standard data processing agreement), but client consents for each data transfer is not necessary.

Myth 4: The right to erasure requires organisations to delete all data about an individual

Fact: The new right to erasure is not an absolute "right to be forgotten". Rather, it is a right to have data deleted if the data is no longer required and in other circumstances where the organisation does not meet the GDPR requirements. If an organisation still legitimately needs to retain the data (for instance due to record retention requirements), then this personal information does not need to be deleted.

Myth 5: The GDPR applies to all universities that have EU students

Fact: Just having students from the EU enrolled is not enough for GDPR to apply. The GDPR generally applies to institutions that are established in the EU. It also applies to universities outside the EU, but only if they offer goods and services to individuals in the EU or monitor the behaviour of individuals in the EU. To be considered "offering services" requires some degree of targeting. The mere fact that EU students are enrolled is not sufficient. The GDPR may, however, apply when universities actively target EU residents (e.g. for online courses) or actively recruit students in EU countries. These criteria are open to interpretation. We recommend that clients obtain their own legal advice.

IMPLEMENTING THE GDPR

Why it is important to get data privacy and the GDPR right

The risk of 4% global turnover fines is certainly a reason why many organisations have started taking data privacy more seriously. But we think that the positive case for good data privacy practices is at least as compelling because data privacy is a human right and having robust data privacy practices creates trust.

In today's society personal information is everywhere. Personal information is often called the new oil of the economy. We all use online services and hand over our personal information. But study after study shows that organisations are not trusted when it comes to personal information. There is a sense that individuals have lost control over their data. Lawmakers and regulators are reacting to this. The GDPR is probably the most prominent example. Organisations need to (re)gain the trust of the individuals. Good data privacy practices are key to build this trust. They are also a competitive advantage. Lastly, they also help organisations with innovation. If students (and staff) trust your institution, they will be more likely to share their information and use new tools.

Getting data privacy wrong can be catastrophic. Data breaches are regularly in the news. What follows is reputational damage, the loss of trust of individuals and the risk of claims from those whose data has been mismanaged. The data protection authorities may not use 4% turnover fines right from the start, but they have many other enforcement tools at their disposal and can force institutions to change their data practices and implement data privacy programs with regular external audits.

Our and your organisation's role under the GDPR

The GDPR maintains the concept of "data controller" and "data processor". This concept is crucial as it determines the responsibilities and liabilities of organisations and their service providers.

An organisation is considered a data controller if it determines the "means and purposes" of the processing of personal information, i.e. why and how personal information is used. The data processor on the other hand is the organisation that acts on behalf of the data controller and under its instruction.

For most of Blackboard's products and services (e.g. Learn, Collaborate, Moodlerooms), Blackboard is considered a data processor and our clients the data controller.

The GDPR imposes more direct requirements on data processors such as Blackboard. However, the majority of GDPR requirements still apply to data controllers (e.g. the responsibility to inform the individuals how their data is being used, to comply with individuals' requests for access to their data, mandatory breach notification to data protection authorities and individuals).

What can you do to prepare for the GDPR?

All organisations in the scope of GDPR will need to ready by 25 May 2018. Here are a few key things that clients can do to prepare themselves. This list of steps is based on our own experience and by no means intended to be comprehensive. Please make sure to engage data privacy experts to help you with your implementation. Many data protection authorities have also created their guidance on how to implement the GDPR.[11]

Hopefully you already have steps 1-6 behind you and are in the middle of implementing your action plans. But it's never too late to start. Even if you have only just started, you can implement the most critical changes. It also means that you will be able to demonstrate to your data protection authority that that you are working on a plan. Ignoring the GDPR is not an option.

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.[12]

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. This project will span across all departments of your institution and you will need help.

3. **Nominate an experienced GDPR lead to manage the project**

   The lead should not just be an experienced data privacy lead, but also 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.

4. **Ensure senior management buy-in and oversight**

   Implementing a GDPR project without the support, direction and oversight of the senior management is difficult.

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

   Understanding where and how personal information is used and where GDPR enhancements are required is the first key phase of the GDPR project.

6. **Develop action plans to close gaps**

   This is probably the hardest part of GDPR as it requires translating the often high-level requirements of the GDPR into specific and practicable actions for all the various processes and systems.

7. **Implement action plans**

   Trust is good, but control is better in this case. This phase requires the tracking of the action plans of others to make sure they are meeting their deadlines.

8. **Review your vendors**

   Under the GDPR you are responsible for your vendors. Having the right contractual provisions in place is important, but not sufficient. You need to be comfortable that your vendors are meeting GDPR requirements and can support you with your compliance. Ask how they are implementing the GDPR.

9. **Stay abreast of legal / regulatory developments (Art. 29 Working Party guidelines, Member States implementing laws)**

   Knowing the GDPR is enough, right? Wrong! While the GDPR applies directly, all EU Member States are implementing national supplementing data protection laws. These are required to regulate areas where Member States have legislative authority (e.g. employee data privacy) or where the GDPR allows them to further legislate (e.g. criteria for DPOs and DPIAs). Additionally, WP29 is publishing important guidance. Keeping up to date is challenging but important.[13]

BLACKBOARD'S PLAN AND APPROACH

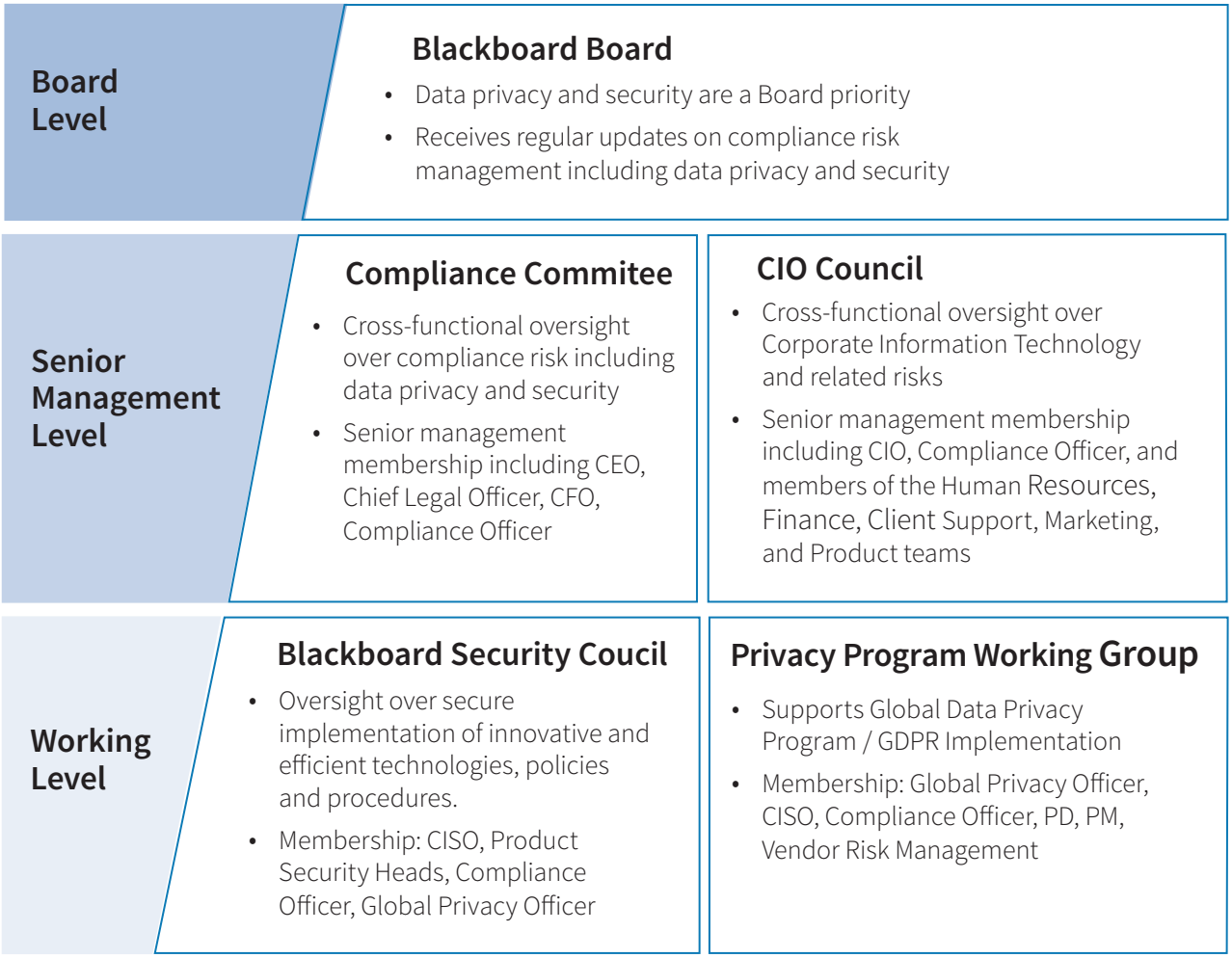
Data privacy and security at Blackboard

Data privacy and security have been a long-standing key priority of Blackboard. For us, the GDPR is an opportunity to further strengthen our existing data privacy practices.

Our approach to data privacy has always been client-focused. We understand the challenges our clients face and want to help you with them.

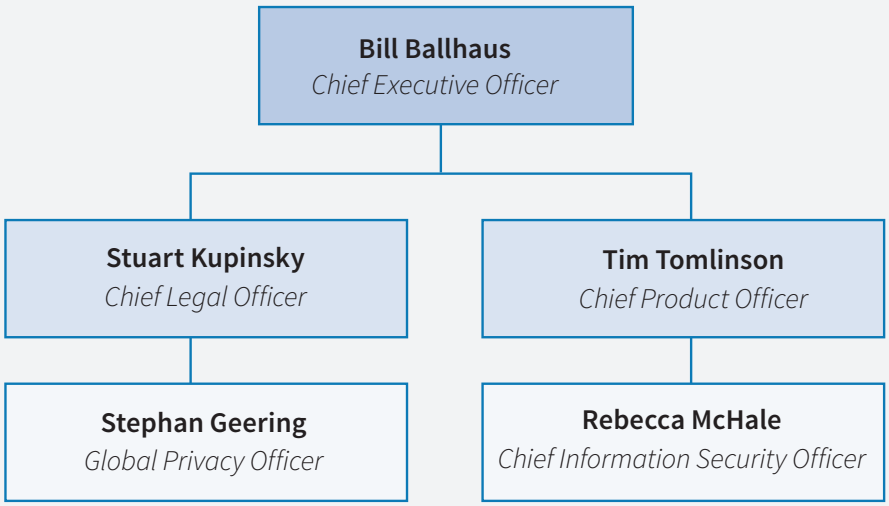
Good data privacy practices require a solid governance model. At Blackboard data privacy and security are a Board priority and our governance model (see below) ensures that senior management oversees and supports our data privacy and security efforts.

The importance that Blackboard places on data privacy and security is also highlighted by the fact that our Global Privacy Officer and Chief Information Security Officer[14] report to the CEO Leadership Team (see organisational chart below)



Privacy and Security

The importance that Blackboard places on data privacy and security is also highlighted by the fact that our Global Privacy Officer and Chief Information Security Officer report to the CEO Leadership Team.



Blackboard's GDPR approach

We have established a comprehensive project to implement the requirements of the GDPR using the following approach:

- The GDPR implementation builds on Blackboard's existing data privacy experience and compliance mechanisms
- The GDPR implementation is led by the 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 GDPR implementation
- The GDPR implementation is overseen by Blackboard's Compliance Committee, which includes the company's CEO, Chief Legal Officer, and other senior officers

GDPR as an opportunity

We think of the GDPR implementation not as a mere effort to comply with new EU data privacy requirements, but also an opportunity. As such, we aim to use the GDPR implementation to accomplish the following:

- Strengthen global data privacy practices – we will use the GDPR project to enhance our global data privacy program in the EU and beyond
- Develop privacy by design processes that further build data privacy compliance into our day-to-day processes
- Support our clients with their GDPR compliance efforts
- Position Blackboard as the recognised data privacy leader in Education Technology

Our implementation plan

We are following Bristow LLP's established 3-phase methodology to implement our Global Data Privacy / GDPR program. This methodology is being used for numerous other companies, including leading technology companies. The three key phases are as follows:

- **PHASE 1 - Information gathering**
- **PHASE 2 - Development of solutions**
- **PHASE 3 - Implementation workstreams**

We have used this 3-phase methodology to develop our program with the following four key stages:

Project Initiation

The project initiation stage included the following activities:

- Senior management briefing and buy-in
- Hiring of a Global Privacy Officer with the responsibility to lead the GDPR project
- Development of project plan and project governance
- Initial information gathering and assessment of current compliance activities for areas requiring enhancements under GDPR

PHASE 1 - Information Gathering (Workshops)

During this initial phase we conducted structured conversations/workshops with key stakeholders from Blackboard's functional areas and product groups to obtain detailed information about data processing practices within those areas.

The output from the workshops was used to perform the gap analysis and develop the solutions and implementation plans in phase 2.

PHASE 2 - Development of solutions

Based on the information from the workshops, we developed the following solutions and documentation:

- Enhanced internal data privacy documentation (policy and detailed operational standards) that reflect the GDPR requirements and explain how GDPR requirements will have to be met for the various data processing activities (e.g. requirements for processing of client data, privacy by design process)
- Product requirements
- Implementation plans for the functional areas and for centrally required efforts

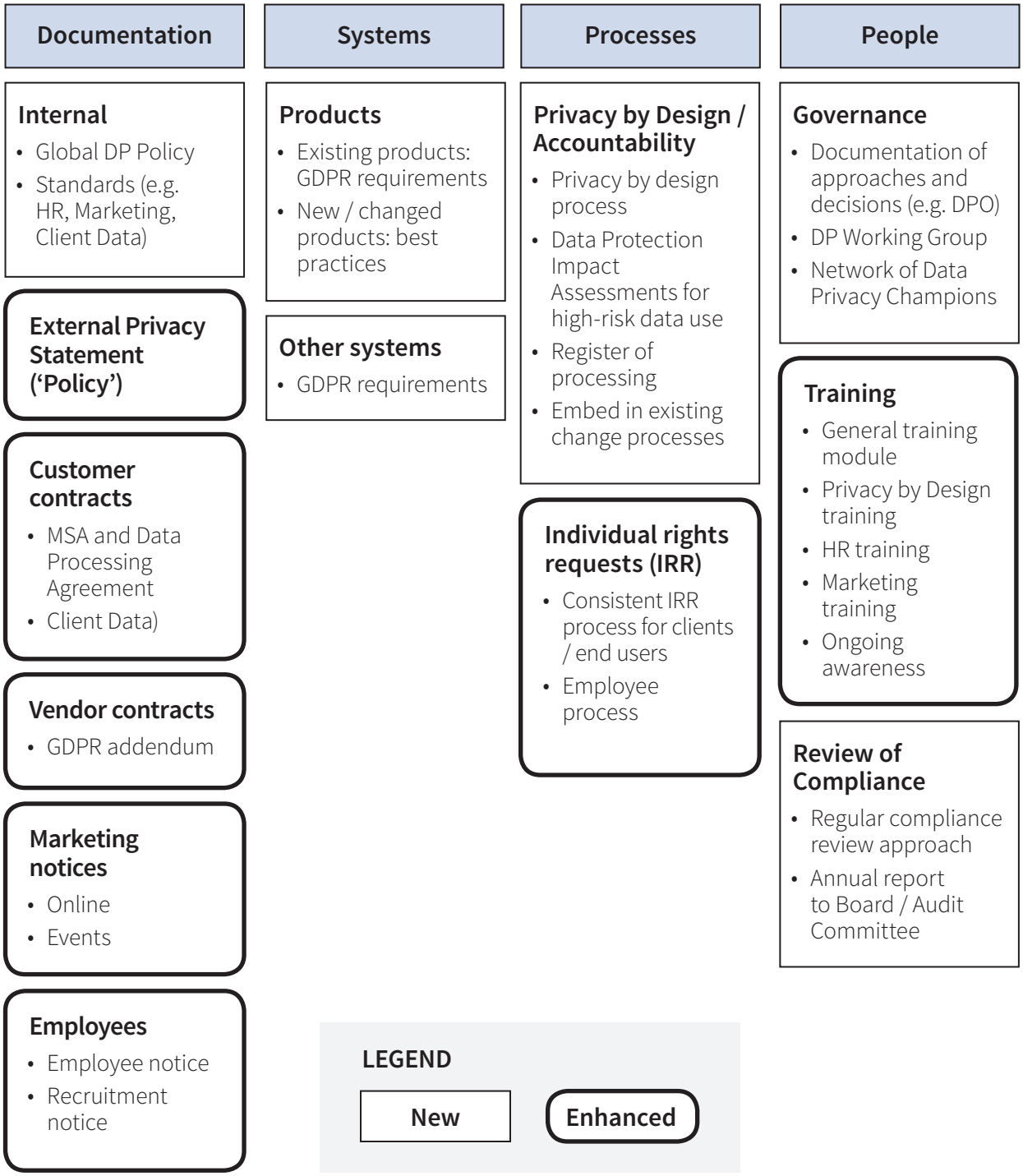
PHASE 3 - Implementation Workstreams

During the final phase, we are implementing the developed data privacy documentation and executing the implementation plans. Six main workstreams will be used to accomplish the implementation:

1. Execute the implementation plans for the functional areas and product groups
2. Review and update of public-facing policies, notices and consents
3. Enhance governance (roles & responsibilities, training, privacy by design etc.)
4. Review and update vendor contracts (where necessary)[15]
5. IT systems changes (where necessary)
6. Establish data processing register

Overview of changes

The chart below shows how we envisage the end state of our GDPR / data privacy program following the implementation activities. After the GDPR implementation we will continue to innovate and adapt to further mature our data privacy practices.



HOW WILL OUR GDPR PROGRAM HELP YOU?

Blackboard's Global Data Privacy / GDPR implementation program is focused on supporting your organisation with your implementation of the GDPR. The following sections will provide more detail, but in summary the key 7 points are:

1. **GDPR-ready products:** We are implementing product requirements to support clients with transparency requirements, individual rights requests etc.
2. **Privacy by design:** We are implementing a privacy by design and Data Protection Impact Assessment (DPIA) process to facilitate the documentation of compliance
3. **Data transfers:** We will continue our multi-layered approach: Regionalisation, EU-US Privacy Shield and EU-approved model clauses
4. **Contract with clients:** We have a GDPR-ready data processing addendum to our standard master agreement
5. **Our vendors:** We have robust contracts and a Vendor Risk Management framework in place
6. **Security:** We have established policy, procedures and governance that are continuously enhanced to safeguard the security of client data
7. **Breach notification:** We have a documented and tested Security Incident Response process

1. GDPR-ready products

Supporting our clients by making our products GDPR-ready is one of the key aspects of our implementation workstreams. To that end, we devised minimum GDPR/data privacy requirements for our products. In line with our approach to strengthen our data privacy practices globally, most of these requirements apply to all our products, not just those products we make available in the EU. This also support our clients outside the EU which may fall into the scope of the GDPR.

We developed our GDPR/data privacy product requirements through a robust and intensive process. We drafted an initial version with external counsel. During multiple working sessions and revisions with key stakeholders from our product development and product management teams we refined the version into specific and actionable general product requirements with detailed guidance. The GDPR/data privacy product requirements were subsequently translated into product-specific actions in the product implementation plans for each product group.

Our product requirements[16] can be categorized as follows:

Transparency

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

Data minimisation / deletion

- Review of products for unnecessary / optional fields
- Review of products for opportunities to use of pseudonymous or anonymous data instead of personal information
- Ability to delete personal information when requested by clients (where clients/ users cannot delete data themselves)

General individual rights

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

EU individual rights

- Ability to deal with data portability requests (right of individuals 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)

Blackboard already has defined programs for our product security that take GDPR into consideration. We therefore did not define additional GDPR specific security requirements.[17]

2. Privacy by design

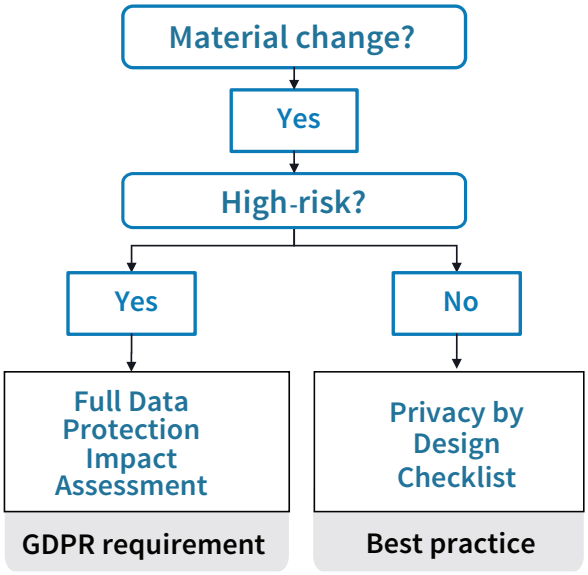
As it becomes more and more challenging in today's world for individuals to maintain control over their information (see our privacy day blog post on this topic), privacy by design and accountability become increasingly important to maintain the trust of individuals, clients and regulators and to document how an organisation complies with the GDPR. We are therefore putting our privacy by design approach at the heart of our Global Data Privacy / GDPR program.

For Blackboard this is an evolution rather than a revolution. We have always conducted legal reviews of new products and practices. With our privacy by design approach we are formalising and better documenting these reviews.

Approach

- We created a documented privacy by design process and checklist.
- Functional areas and product groups are including the privacy by design checklist into their change processes.
- Every material change in how personal information is used requires completion of the privacy by design checklist. While not specifically required by the GDPR, this is best practice.
- The checklist will trigger the more detailed Data Protection Impact Assessment (DPIA) for high-risk use of personal information (GDPR requirement)

The flow chart below visualises the approach:



3. Data transfers

The GDPR does not bring any significant changes to how personal information can be transferred outside the EU/EEA. The current restrictions and data transfer mechanisms remain. This means that data transfers are allowed if an EU approved data transfer mechanism such as the EU-US Privacy Shield or the EU-approved model clauses (data transfer agreements) are in place. These mechanisms ensure that personal information is adequately protected even when leaving the EU/EEA.

We will continue our multi-layered and redundant approach to data transfer compliance. This means we address the data transfer requirements via multiple avenues to ensure proper safeguards are in place for your information:

- **Regional hosting:** We have a regional hosting strategy with almost all products hosted in the EU and other products planned to be moved to regional hosting solutions. While regional storage is not required by the GDPR and we do not think that data localisation leads to better data privacy or security,[18] we understand that many EU clients prefer their data to be stored in the EU.
- **Privacy Shield:** Blackboard is EU-US Privacy Shield certified which allows us to lawfully transfer personal data to the US.
- **Model clauses:** We also use EU-approved "model clause" agreements that allow us to compliantly transfer personal data outside the EEA within Blackboard's group of companies ("Customer Data Transfer Agreement").
- **Vendors:** Robust contracts are in place with vendors and partners (e.g., IBM, Amazon Web Services) to ensure that data transfer requirements (and other data protection obligations) are passed on to our vendors and partners.

We currently[19] have several regional data centers to support data handling in the EU for our EU clients:

- Managed hosting (Blackboard data centers): Data centers in Amsterdam (the Netherlands) and Frankfurt (Germany).
- Cloud hosting (AWS data center): AWS region Frankfurt, Germany (eu-central-1).

AWS data centers meet a host of certifications and requirements from ISO 27001 and ISO 27018, to SOC2 and to compliance with GDPR as well as compliance with local requirements such as the German C5 and IT-Grundschutz.[20]

It is important to understand that while personal information of clients is stored in these data centers for most of the products (including Learn 9.1, Learn SaaS, Moodlerooms and Collaborate) for EU clients, access to this data from outside the EU/EEA may be required to provide the products and services, e.g. for 24/7-support. Such data transfers are allowed thanks to the mentioned EU-US Privacy Shield certification and model clauses.

4. Contracts with clients

The current Directive requires a data controller to have a contract in place with the vendor (data processor), but does not prescribe the content of the contract in detail. The GDPR is more prescriptive and includes a list of required content.[21]

Our current standard data processing addendum includes all the required points below. It is automatically included for clients on our standard master agreement who are in scope of the GDPR.

- ✓ Use personal data only as instructed
- ✓ Staff must sign confidentiality agreements
- ✓ Appropriate security measures need to be in place
- ✓ Only engage 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
- ✓ Return or delete 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

5. Managing our 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.

As part of our GDPR program we are closely connecting the privacy by design approach with the existing Vendor Risk Management and Procurement processes. This results in the following key controls:

- Robust contracts with a Privacy and GDPR Addendum in place with third parties imposing materially equivalent provisions that we have in place with our clients
- "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

6. Security

The GDPR does not materially change the technical and operational measures ("TOMs") for the security of personal information. Such measures need to be "appropriate" to the risk involved as under the current Directive. We therefore continue to rely on our established information security programs.

Governing information security risk

We have established policy, procedures, governance and technical requirements to manage IT security risk across the business.

From day one, Blackboard staff must understand their responsibility to protect client personal data:

- Acknowledge policy to protect sensitive information
- Annual user security and data privacy training
- Phishing exercises
- Awareness bulletins

The following requirements are in place for the protection of data by our staff:

- Data classifications are defined with requirements to protect each data type. Of highest sensitivity is our client's data – the data of the institutions and their learners.
- Technical controls are in place to safeguard data, e.g.:
  - use of encryption
  - prompt security updates
  - enhanced authentication controls
  - malicious email & web traffic protection
  - endpoint protection technologies
  - access restricted based on need-to-know

It's not just the GDPR …

As a global company, serving the education community, we closely monitor relevant geographic and education-sector specific data privacy and security laws and regulations.

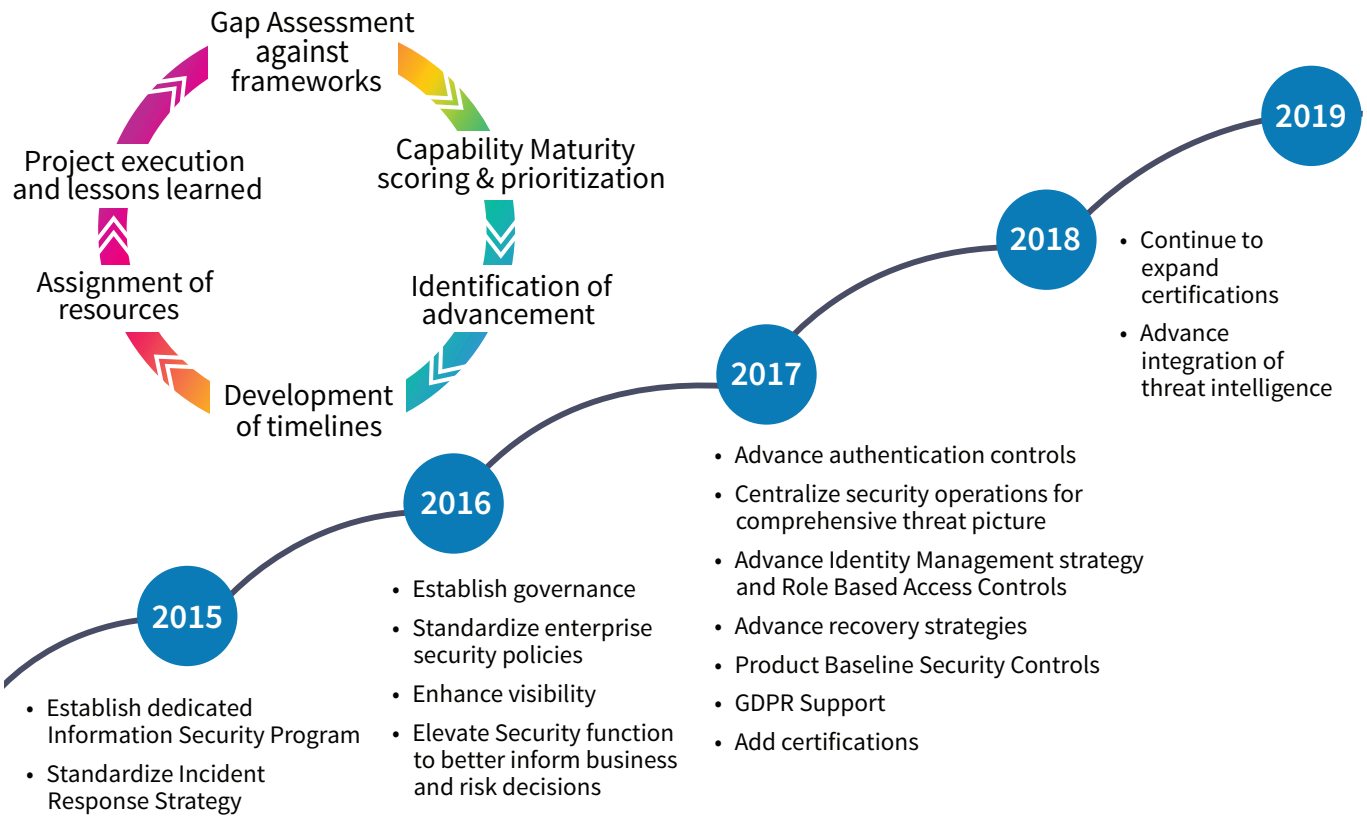
The list below are just some examples of security and data privacy regulations, standards and frameworks Blackboard takes into consideration in addition to GDPR when developing our security policies, processes, and technical controls.

- US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
- US Children's Online Privacy Protection Act (COPPA)
- US State Laws (existing and emerging 50-state patchwork)
- US Government standards – FedRAMP
- PCI Data Security Standards, where applicable
- ISO/IEC, OWASP, NIST
- International standards (MTCS, IRAP)

Security maturity assessments & roadmaps

We work hard to continuously enhance our technical and operational security measures. The diagram on the next page visualises our continuous maturity assessments and our roadmaps.

Adopting Frameworks: Security Maturity Assessments & Roadmaps



7. Breach notification

One of the key changes of the GDPR is the new mandatory notification of personal data breaches to the competent data protection authority and (in some cases) to the affected individuals.[22]

For most of our products and services, Blackboard is a data processor[23] under the GDPR. The obligation to notify data protection authorities and individuals in case of a breach that involves Blackboard would therefore lie with our clients. However, the GDPR requires data processors such as Blackboard to notify their clients (data controllers) without undue delay (i.e. "promptly")[24] in such a case.

We have the following measures in place that support our clients meeting their obligations in the event of a personal data breach at Blackboard related to a client:

- Blackboard's 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)
- Our obligation to notify clients promptly is expressly stated in our current standard master agreement and data protection addendum[25]

CONCLUSION

The GDPR requires significant changes with impact beyond the compliance date of 25 May 2018. We hope that this white paper can contribute to your successful implementation of the GDPR and has demonstrated how seriously Blackboard takes the GDPR and data privacy compliance.

The next sections provide additional helpful information and list our contact email if you have any questions or feedback on this white paper.

HELPFUL GDPR RESOURCES

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

For detailed analysis on how the GDPR applies to you, you should also seek the advice from specialists. It is important to rely on experienced data protection experts (e.g. from your law firm of choice).

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 with helpful material in simple language that is constantly updated
- 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 (and much more material in French language)
- The Spanish AEPD produced a guide for educational institutions (PDF, in Spanish)

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

BIOGRAPHIES

Stephan Geering

Global Privacy Officer

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

Stephan's 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)
- CIPP/E certified

Rebecca McHale

Chief Information Security Officer

- Leads security strategy for products and infrastructure
- Oversees Blackboard cybersecurity governance
- Reports to Chief Product Officer
- Based in Washington, D.C.

Rebecca's background:

- Joined Blackboard in 2106; recently combined security teams and elevated role of security organization within company
- MS Discrete Mathematics and Computing Applications at Royal Holloway, University of London
- Previously Senior Director for Cyber Programs at Novetta and CSRA serving US government and commercial clients – e.g., Department of State, Transportation Security Administration (TSA), and Federal Deposit Insurance Corporation (FDIC)

MORE INFORMATION

You can find more information on our dedicated Data Privacy and Security Community page.

We also have a Data Privacy Newsletter. If you would like to receive our newsletter or have any questions or feedback regarding this white paper, please contact us at privacy@blackboard.com.

Sources

1 See the "Helpful GDPR resources" section at the end for more detailed guidance on the GDPR.

2 We prefer the term "personal information" to "personal data" but use it with the same meaning and scope as "personal data".

3 The data controller is the organization that determines the means and purposes of data processing (how and why personal information is used).

4 See section "Our and your organisation's role under the GDPR.

5 See section "Demystifying the GDPR" below for more details on data transfers.

6 See the ICO's "An introduction to the Data Protection Bill" for a helpful overview of the bill.

7 See also the UK ICO's blog posts about GDPR myths.

8 See also the WP29 (draft) Guidelines on Consent under Regulation 2016/679 (WP259) and the ICO's guidance on consent.

9 WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01).

10 See also section "Data Transfers".

11 See for instance the UK ICO's Preparing for the GDPR – 12 steps to take now (PDF).

12 See also section "Demystifying the GDPR".

13 See section "Helpful GDPR resources".

14 For more information on the Global Privacy Officer and Chief Information Security Officer see the Biography section.

15 As part of the EU-US Privacy Shield certification project, we already included the necessary GDPR contract provisions in many of the contracts with our vendors (sub-processors) that have access to EU personal information.

16 Please note that not all product requirements apply to all products. For instance, some products do not have a user interface that would allow for clients to link to their privacy policies/notices.

17 See section "Security" for more details.

18 Once a network or system is connected to the internet, the physical location of data has little to no impact on security threats. See Amazon Web Services (AWS) white paper "Data Residency AWS Policy Perspective" (particularly pages 2 and 3) for compelling arguments against data localisation.

19 As of the date of this document.

20 See AWS Compliance Programs for the full list of certifications and legal compliance.

21 Art. 28(2)-(4) GDPR.

22 Art. 33 and 34 GDPR.

23 For an explanation of the role of the data processor see the section "Our and your organisation's role under the GDPR".

24 See the section "Demystifying the GDPR" above for more details on the timing and process of personal data breach notification

25 See also section "Contracts with clients".

Blackboard.com