Blackboard®

DATA PRIVACY PRODUCT REQUIREMENTS

Version 1.0

Date	Version	Description / Changes	Author
12/07/2017	1.0	Initial version.	S. Geering

Blackboard Internal - Not to be shared externally

Please note that this document will continue to be updated. While the requirements will not change, we will continue to update the guidance based on feedback and requests where appropriate. The latest version will be available in our Yammer group and changes to previous versions will be highlighted. We will also make stakeholders aware through our GDPR distribution lists. Please send any comments and feedback to stephan.geering@blackboard.com*.*

A. Introduction

1. Scope and purpose

This document defines the product data privacy requirements **globally (and not just for the EU)**. It applies to all information systems (computing devices, applications, databases and supporting network infrastructure) made available to clients as a product or service, which include Personal Information (Client Product Systems). For the definition of Personal Information see below under 2.

The document was developed in cooperation with PD/PMM management as well as the Architecture and Product Design teams.

The document should enable each owner of a Client Product System to understand the minimum IT requirements necessary for Blackboard to comply with its data privacy obligations and to support clients with their obligations. It provides additional guidance on each of the requirements in this document and the related actions in the product specific implementation plans. We will also develop best practices for new / changed systems going forward that will go beyond the minimum requirements with the aim to assist our clients in meeting their data privacy obligations in more systematic ways.

This document is divided into three sections.

- Section B provides the list of all requirements.
- Section C provides the detailed guidance for all systems in scope
- Section D provides the detailed guidance for those systems that are in scope for the EU General Data Protection Regulation (GDPR)

2. Definition of Personal Information

The scope of the requirements below is closely linked to the definition of "Personal Information". It is therefore crucial to understand the definition and scope of what is considered Personal Information.

While the definition of Personally Identifiable Information (PII) under some US laws can be more narrow, in the EU and most countries around the globe, the definition of Personal Information ("or personal data") is **very wide** and includes data that may not intuitively be considered Personal Information. It basically encompasses any information about an identifiable individual and any information that is linked to such an individual. Even if such information is publicly available.

Blackboards' definition of Personal Information is aligned to this globally concept of Personal Information. The official Blackboard definition with examples is available on the intranet and included here for ease of use:

> *"Any data relating to an identified or identifiable natural person. This can include (but is not limited to) names, email addresses, photographs, job applications, online access credentials, purchase history, account information, personnel files (in paper or digital format), occupational health records, opinions, and correspondence to and from an individual."*

Identifiable means that the individual can be identified by the data itself (even if there is no obvious identifier such as a name or SSN) or by combining the data with data that is reasonably available. For instance, if a Client Product System only uses a student ID number (provided by the client or us) and no other direct identifiers such as a name, that data would still be considered Personal Information if the client and/or Blackboard has access to the separate database that links the student ID number back to the name / identity of the student. Similarly, such data would be considered Personal Information if the individual could be identified based on the richness of information included in the Client Product System (e.g. by the combination of DOB, gender, subscribed courses, grades etc.) or when it is combined with reasonably available information (e.g. information available on the internet).

What does this mean in practice?

Content that due to its nature and purpose is likely to include Personal Information such as the content of assignments, messages/posts/chats/blogs, notifications, survey and quiz responses, notes made by the students/users, submitted work, chat or audio recordings of sessions and classroom discussions (e.g. in Collaborate) as well as outcome of analytics about a user (e.g. progress or retention risk reports) would generally be considered Personal Information of those users.

Conversely, content that due to its nature or purpose is unlikely to include personal information, such as course material uploaded by institutions would generally not be considered Personal Information.

Information on how a student / user uses a system (e.g. a student's login time would be considered Personal Information. Aggregate information that does not identify an individual (e.g. 27 students of class X have attended a session) is not considered Personal Information.

Blackboard Internal - Not to be shared externally

B. Overview of requirements

#	Principle	Requirement description	Scope
1	Data Security	Client Product Systems need to comply with the Product Baseline Security Controls (PBSC) framework which defines the commercially reasonable security controls (and exemptions where appropriate).	Global
2.1	Transparency	Client Product System can make available / link to the privacy notice of the client during login of the end user and should include a consent mechanism.	Global
2.2	Transparency	Client Product System has the ability to display a link to a client privacy notice when the user is logged into the system (e.g. in the Settings or Help Menu)	Global
2.3	Transparency	A repository is available for clients to store their privacy notices (to allow for 2.1 and 2.2)	Global
2.4	Transparency	Client Product System provides general information (directly in the system or via a link to another Blackboard document / website) how the System / Blackboard uses Personal Information	Global
3.1	Data Minimisation / Deletion	Review Client Product System for unnecessary and optional data fields. Remove unnecessary fields and make fields optional (and mark them as such) where appropriate.	Global
3.2	Data Minimisation / Deletion	Review Client Product System to determine if 'pseudonymous', 'de-identified' or 'anonymous' data can be used instead of Personal Information and make changes where appropriate.	Global
3.3	Data Minimisation / Deletion	Approach is in place and documented to allow for Personal Information to be deleted, restricted or anonymized (completely and/or for specified user accounts) when no longer required or as requested by the Client.	Global
3.4	Data Minimisation / Deletion	Develop and maintain guidance for client admins on which fields and functionalities regarding Personal Information are required and which are optional.	Global
4.1	Individual rights	Approach is in place and documented for Client Product System to be searched to find all the data relating to a user within a reasonable time period if requested by client.	Global
4.2	Individual rights	Approach is in place and documented that allows for all data related to a user to be made available to Client and/or user within a reasonable time period retained (where Blackboard system is 'system of record').	
4.3	Individual rights	Approach is in place and documented for Client Product System to allow for user data to be corrected and deleted within a reasonable time period if requested by client (where Blackboard system is 'system of record')	Global
4.4	Individual rights	Approach is in place and documented that allows for a record of the correction to be added to / referenced in the Client Product System within a reasonable time period where a record of the initial information needs to be retained (where Blackboard system is 'system of record')	Global
4.5	Individual rights	A list of third party suppliers with access to the Client Product System must be created and maintained (including description of their role and access locations).	Global
4.6	Individual rights	Client Product System must maintain a log file of actions taken on the account related to individual rights, so that it is possible to audit the actions which were taken and when. Where not in place, actions taken on the account need to be documented in another available document (e.g. the relevant support ticket)	Global
5.1	EU rights	Approach is in place and documented that allows for all data related to a user to be extracted and provided to the client / user in a commonly available, structured and machine-readable format (e.g. CSV) within reasonable time period if requested retained (where Blackboard system is 'system of record').	EU*
5.2	EU rights	Approach is in place and documented that allows to stop actively collecting / using information about a specific user where requested, so that no changes take place for that data (with the consequence that the user will no longer able to use the system) (e.g. through export/removal of data) retained (where Blackboard system is 'system of record').	EU*

* **Please note**: Such EU GDPR requirements can also apply to Blackboard where a client outside the EU provides products and services to EU residents (e.g. by actively advertising and providing online courses to EU residents) (see section D).

Blackboard Internal - Not to be shared externally

C. Global requirements

1. Data security

Goal: The GDPR and most data privacy laws do not specify security requirements in detail, but require security measures to be appropriate. Client Product System must therefore have security measures which are **appropriate** to the nature of the data and the risks to that data. The more sensitive the information and the more likely it will be at risk of unauthorised access, the stronger the security measures should be.

Requirement 1: Client Product Systems need to comply with the Product Baseline Security Controls (PBSC) framework which defines the commercially reasonable security controls (and exemptions where appropriate).

Guidance: The PSBC framework has been developed with the involvement of the Global Privacy Officer to define the 'appropriate' or 'commercially reasonable' security controls for systems that are provided to clients. During the development of the PBSC, the GDPR requirements have been taken into consideration.

The GDPR does not define which security controls are appropriate in which situation, but leaves it to organisations to make this determination based on the risk. The GDPR (in Art. 32(1)) clarifies that this determination should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of using Personal Information as well as the risk of varying likelihood and severity of using Personal Information (particularly regarding the risk from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Information transmitted, stored or otherwise processed).

The PBSC allows for justified exemptions and the exemption process includes review by the Global Privacy Officer / Legal which will take GDPR requirements into account. An approved PBSC exemption therefore does not require an additional exemption under the Global Data Privacy Policy.

2. Notice and Transparency

Goal: The Client Product System should allow individuals to understand how their Personal Information is being processed when they use the system ('privacy notice'). It is generally the obligation of the client (as the data controller) to provide this information rather than the obligation of Blackboard. The Client Product System should therefore have the functionality for the client to provide the users with information describing the manner in which the client intends to use Personal Information. This is achieved through the following requirements.

Requirement 2.1: Ensure Client Product System can make available / link to the privacy notice of the client during first login of the end user and should include a consent mechanism.

Guidance: This requirement is not applicable where the Client Product System is integrated in another system and doesn't have a user login / interface since the system is launched through another application (e.g. the LMS). In this case reliance is placed on the underlying system (e.g. LMS) to make this functionality available.

Where the requirement applies, the Client Product Systems need to at a minimum be able to link to a privacy notice. This link should be made available at the first time a user logs in and

Blackboard Internal - Not to be shared externally

at subsequent log-ins (e.g. on the log-in screen). Where Blackboard is a data processor[1], the client needs to be able to link to his own privacy notice. If the client does not use the functionality, there should be a placeholder notice that explains that the client did not provide a privacy notice and that the end user should contact the client to obtain it (e.g. "Your institution has not provided a link to its privacy policy / notice. You should be able to find your institution's privacy policy / notice on its website.")

This could be achieved by allowing the client admin during the configuration to provide a link to the client's privacy notice.

Obtaining consent has become more difficult in the EU under the GDPR because it needs to be 'freely given' (which is doubtful if users cannot choose if they want to use a system or not). Many EU clients are therefore unlikely to rely on consent (but rather on another legitimate ground to process Personal Information). However, some EU clients may still want to rely on consent and in many other countries consent is still the main legitimate ground to process Personal Information. Systems therefore should (as best practice) be able to provide the client with an option for the client to obtain consent (e.g. by using a consent tick box or "I agree" button) and retain evidence that the user consented.

Requirement 2.2: Client Product System has the ability to display a link to a client privacy notice when the user is logged into the system

<u>Guidance:</u> This requirement is not applicable where the Client Product System is integrated in another system and doesn't have a user login / interface since the system is launched through another application (e.g. the LMS). In this case reliance is placed on the underlying system (e.g. LMS) to make this functionality available.

Where the requirement applies, the link should be reasonably prominently placed so that the user can find the link to the privacy notice without having to step through too many menus / steps. This could for example be in the user profile or in a settings or help menu. It needs to be very clear that this is the client's privacy notice from the link / description.

Requirement 2.3: Make a repository available for clients to store their privacy notices (to allow for 2.1 and 2.2)

<u>Guidance:</u> This requirement is not applicable where the Client Product System is integrated in another system and doesn't have a user login / interface since the system is launched through another application (e.g. the LMS). In this case reliance is placed on the underlying system (e.g. LMS) to make this functionality available.

Where the requirement applies, clients may require Blackboard to store the privacy notice in a repository for them. While we expect that most clients would provide a link to the privacy notice on their website, Blackboard needs to be able to accommodate such requests.

[1] For the definition of data controller and data processor and the related categorisation of the products please refer to the clients Data Standard.

Requirement 2.4: System provides general information (directly in the system or via a link to another Blackboard document / website) how the System / Blackboard uses Personal Information

Guidance: This is a separate document from the privacy notice mentioned under 2.1-2.3 and is not a legal document. Using a standard template (which will be provided by Global Privacy Officer/Legal) the document explains from Blackboard's perspective how the system generally uses personal information (and will refer to the client's privacy notice for information on how the client specifically uses the data).

3. Data minimisation and deletion

Goal: The Client Product System should only process the minimum Personal Information necessary to achieve its purpose. It should therefore make the provision of not strictly necessary Personal Information optional. Pseudonymous, de-identified or anonymized data should be used if Personal Information is not needed. Personal Information that is no longer required (by the client) should be deleted.

Requirement 3.1: Review Client Product System for unnecessary and optional data fields. Remove unnecessary fields and allow clients to make fields optional (and mark them as such) where appropriate.

Guidance:

The review for unnecessary fields should focus on data fields that are clearly not necessary or useful for any client.

Data fields that are required for meeting certain standards (such IMS' interoperability standards or other industry standards that the Client Product Systems is subject to or adheres to), are considered necessary. Equally, where data fields are connected to other fields and cannot be removed without impacting the system architecture or logic, those fields are considered necessary.

The determination on which fields are necessary depends on whether Blackboard is considered a controller or processor:

- *Data controller: Where Blackboard is a data controller it can determine itself which fields are required for its use and can therefore conduct this review independently.*
- *Data processor (most products): For Client Product Systems where Blackboard acts as a data processor, the client ('data controller') determines which data field are being used by them and necessary for them, so it is challenging for Blackboard to determine which fields may be considered (un)necessary by the Client. The review should focus on whether there are any data fields that are clearly not necessary or helpful to provide the system functionalities to any of the clients.*

A possible outcome of the review is that all existing data fields are necessary. The key is that the review is conducted and its outcome documented. Data fields identified as unnecessary should only be removed after discussion and agreement with all relevant stakeholders.

The review for 'optional' fields should identify those fields that are not necessary for using the core product / service functionalities and could be made optional by the client.

Therefore, if data fields would be helpful (for Blackboard or the client) for delivering the product or service, but are not strictly necessary for the core functionalities, the data field should be considered optional and the client (admin) should have the ability to make them optional and mark them as such. This applies both to data fields that are collected directly from the end user (e.g. user contact details in a form) and to those obtained through the integration with other client systems (e.g. SIS). This should preferably be indicated in the system itself, alternatively in the guidance required as part of 3.4.

The outcome of the review and any resulting changes must be documented.

Requirement 3.2: Review Client Product System to determine if 'pseudonymous', 'de-identified' or 'anonymous' data can be used instead of Personal Information and make changes where appropriate

Guidance: In many cases, providing the products and services will require that users are identifiable in the Client Product System. However, where possible, the Client Product System should use 'pseudonymous' data, 'de-identified' or 'anonymous' data instead of fully identifiable Personal Information.

- *Pseudonymous data is information from which direct identifiers (e.g. name, social security number, student ID number) have been eliminated or transformed, but indirect identifiers (data that helps identify an individual such as date of birth) remain intact.*
- *De-identified data is information where direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.*
- *Anonymous data is information where direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification of the individual.*

More information on these categories can be found in the Future of Privacy Forum's Visual Guide to Practical Data De-identification.

If providing the products and services or one particular aspect of it can be achieved without direct or indirect identifiers (e.g. the individual's name, email address), the Client Product System should not require such information.

The Client Product System should therefore be reviewed for aspects and opportunities where pseudonymous, de-identified or anonymous data can be used if this does not impact the provision of the product or service to the clients and users (e.g. usage analysis, system performance monitoring). According changes should be made where appropriate.

The outcome of the review and any resulting changes must be documented.

Requirement 3.3 Approach is in place and documented to allow for Personal Information to be deleted, restricted or anonymized (completely and/or for specified user accounts) when no longer required or as requested by the client.

Guidance: A systematic solution to automatically delete, restrict or anonymize data after a certain defined retention period is not necessarily required (but best practice). At a minimum an approach needs to be developed (and documented) to allow for Personal Information to be

deleted, restricted or anonymized in line with the retention period (defined by the client) or based on a specific request of one or multiple users' Personal Information. The clients' retention periods may vary by client and may start once an account has become inactive, a student has left the institution etc. The Client Product System should therefore be able to identify accounts / data that have been inactive / closed, so that retention periods can be applied and the relevant accounts deleted.

Quite often, the client has a choice under the service contract to ask for the data to be returned at the end of the contract period. Once the data has been returned and safe receipt has been confirmed, the data will need to be deleted, restricted or anonymized as below.

Restriction (rather than deletion) may be requested where the data is no longer needed for the Client but need to be retained purely for legal purposes.

If the data will be deleted, the deletion should be to a reasonable level of permanence (taking account of the costs involved and the risk of it being reconstituted). For example, the data should be de-indexed from relevant servers or operating Client Product Systems and marked for overwriting. Data deletion for Blackboard Confidential Data (see definition here), may require additional scrutiny and safeguards, such as multiple overwrites of data and the use of industry standard data deletion technologies.

- *If the data will be **restricted** (i.e. where you are required to store data only but not permitted to process for any other purposes), it should be subject to enhanced access controls such that it can be accessed only by a limited number of administrators and its use severely restricted.*

- *If the data will be **anonymised**, it should be permanently anonymised such that it would not be possible to re-identify the individual even with additional reasonably available data, i.e. it should be irreversible. (see above under 3.2 for the definition of "anonymous")*

Requirement 3.4: Develop and maintain guidance for client admins on which fields and functionalities regarding Personal Information are required and which are optional.

Guidance: This guidance is required for the client (as the data controller) to determine which field are necessary for using the product / service and which are optional for their use. This allows them to instruct their users what information they need to provide and which functionalities could be considered optional rather than mandatory. This is required for the client to be in control of the use of Personal Information.

4. Individual Rights

Goal: In the EU and in many other jurisdictions around the world individuals have certain rights regarding their Personal Information, such as the right to access and correct their information. These individual rights requests will (and should) generally be directed at our clients (as the data controllers). The clients will ask Blackboard to support them with those requests. We therefore need to ensure that our Client Product Systems allow us to assist clients with such requests.

Most countries have defined periods to respond to such requests and in the EU such requests must generally be responded within one month. As the client will receive these requests and

will require time to analyse the request before contacting Blackboard for assistance and also require time to review documents / decisions once Blackboard provided them, it is anticipated that clients would request us to deal with such requests within two weeks or less.

Blackboard has not received many such requests in the past. While there may be an increased awareness with the implementation of the GDPR of such rights in the EU we do not expect a significant increase. If this assumption proves wrong, more systematic ways to deal with these requests will need to be developed.

Please note – All of these rights have limitations and exceptions, so it is important that such requests are referred to the Global Privacy Officer / Legal for review before any work starts.

Requirement 4.1: Approach is in place and documented for Client Product System to be searched to find all the data relating to a user within a reasonable time period if requested by client.

Guidance: To assist clients with any individual rights requests, all Personal Information related to a specific user needs to be able to be located in the first place (see above under 1.B. for the definition of Personal Information). Some Client Product Systems may not link all Personal Information directly to the user's ID/account. The information may be connected to various databases (e.g. SIS-connected information, course activity-related information, analytics information) and there may not be a single mechanism to locate all the Personal Information of one specific user. However, at a minimum an approach needs to be identified, set up and documented on how such data can be found within the various databases of the Client Product System.

While IT log files may also include Personal Information in the strict sense (e.g. information in Apache logs linked to a user), Blackboard's position is that such information is not in scope for individual rights requests unless specifically requested.

Similarly, transitory temporary information that is only briefly stored in a system before being stored in another, more permanent system environment and deleted once stored in the permanent system environment, would not be considered in scope for such requests unless specifically requested and still available..

While the individual rights can extend to archive and back-up data, Blackboard's position is that unless specified in the request we would provide Personal Information that is actively used on live / production systems and would not include archive / back-up in the scope of such requests. The rationale is that the main purpose of the individual rights is that individuals can have control over their information that is being used by an organisation and prevent the data use from having a negative impact on them. Information stored on archives and back-up tapes that are not actively used anymore and where the only activity is to store the data is unlikely to have any impact on the individual. However, if the request specifically includes back-up and archive data or if the requests relates to a user whose data is not on the live / production system anymore but only on archive / back-ups, then this may have to be provided (after assessment from Global Privacy Officer/Legal).

A 'reasonable time period' is generally 1-2 business days as the located data will need to be provided, corrected, erased etc. and reviewed by the Global Privacy Officer / Legal before being provided to the client and all of these activities are likely to be required within 14 days or less as explained above.

Requirement 4.2: Approach is in place and documented that allows for all data related to a user to be made available to client and/or user within a reasonable time period retained (where Blackboard system is 'system of record').

<u>Guidance:</u> The documented approach needs to ensure that once data is located it can be made available to the client / user. This does not have to be in electronic format and can be provided as hardcopy print-outs. This right can sometimes be fulfilled by just describing what information is included rather than providing the data itself, but a client may insist that the data itself is provided to the user. Global Privacy Officer/Legal review is required before any data is provided to the client.

A reasonable time period is likely to be 5 business days to ensure there is sufficient time for Global Privacy Officer/Legal review.

Requirement 4.3: Approach is in place and documented for Client Product System to allow for user data to be corrected and deleted within a reasonable time period if requested by client (where Blackboard system is 'system of record')

<u>Guidance:</u> Individuals must be able to correct factually inaccurate data and complete incomplete data in the Client Product System where Blackboard is the 'system of record' (note that this would not apply to mere differences of opinion).

Where another system than the Client Product System is the 'system of record' (gold copy of information, e.g. the client's SIS), then the client will need to correct or delete the requested information. Where Blackboard is the system of record, then Blackboard will need to assist the client with such a request. The rights to have data corrected or deleted are not absolute. Where data is still required, it does not need to be deleted. Similarly, for the right to correct data. The approach therefore needs to ensure that this can take place if requested (and approved by Global Privacy Officer/Legal).

A reasonable time period is likely to be 5 business days once approved by Global Privacy Officer/Legal.

Requirement 4.4: Approach is in place and documented that allows for a record of the correction to be added to / referenced in the Client Product System within a reasonable time period where a record of the initial information needs to be retained (where Blackboard system is 'system of record')

<u>Guidance:</u> If Blackboard or the client needs to retain a record of the initial information (e.g. because it was a contemporaneous report), it should be possible to add or reference a record of the correction.

A client may therefore request us to add/reference a record of the correction in the system and a (documented) approach to allow for this needs to be in place. Ideally, the record would be included in the system itself, but can also be stored in another repository as long Blackboard / the client can easily retrieve the record of correction. As above, such request s need to be reviewed / approved by Global Privacy Officer/Legal.

A reasonable time period is likely to be 10 business days once reviewed / approved by Global Privacy Officer / Legal.

Blackboard Internal - Not to be shared externally

Requirement 4.5: A list of third party suppliers with access to the Client Product System must be established and maintained (including description of their role and access locations).

Guidance: As part of the right to access, individuals also have the right to understand if and which third parties potentially have access to their Personal Information. Such information is also required as part of the Data Processing Addendums that Blackboard has in place with its EU clients. Such a list therefore needs to be maintained with a brief description of their role / purpose of their access to the data and the locations from which the third parties access the system. This list could be referenced in the documentation that is required under the PBSC program and will also be required in the Art. 30 Processing Register that will be developed as part of the Global Data Privacy Program / GDPR Implementation.

Requirement 4.6: Client Product System must maintain a log file of actions taken on the account related to individual rights, so that it is possible to audit the actions which were taken and when. Where not in place, actions taken on the account need to be documented in another available document (e.g. the relevant support ticket).

Guidance: This log file should document where Personal Information has been updated/corrected, deleted or accessed / provided for data portability following an individual rights request. This does not mean that all the historic Personal Information (e.g. deleted account information) needs to be maintained. It should be sufficient to record the action taken (i.e. x field updated), and not the change itself. Ideally, this could be recorded in the system. Alternatively, the changes should be documented in another document that can be made available if required (e.g. the relevant support ticket where it).

D. EU requirements / rights

Goal: The GDPR includes additional rights that go over and beyond the above listed globally recognised individual rights. The two requirements below help ensure that we can accommodate such requests.

The two requirements only apply where systems are in scope of the GDPR (or legislation that provides for the same or similar rights of data portability and right to restrict processing). For most products (i.e. where Blackboard acts as a data processor), the applicability depends on whether the client is in scope of the GDPR. A client can be in scope of the GDPR because it (or more precisely: its main establishment) is located in the EU (e.g. its head office is in the Netherlands). Additionally, a client outside the EU is also in scope where it provides products and services to EU residents (e.g. a US institution actively offering online courses to EU students).

In the rare cases where Blackboard is a data controller, the GDPR applies if Blackboard actively offers the product and service to EU residents (e.g. by having pages in local language, allowing payment in local currency).

The GDPR does not apply by the mere fact that products and services are accessible in the EU. This is a grey area and advice from the Global Privacy Officer / Legal should be sought.

Requirement 5.1: Approach is in place and documented that allows for all data related to a user to be extracted and provided to the client / user in a commonly available, structured and machine-readable format (e.g. CSV) within reasonable time period if requested retained (where Blackboard system is 'system of record').

Guidance: This right is an enhanced version of the right to access (see 4.2) and is intended to allow an individual to use his Personal Information with another service provider. The main purpose is to allow individual customers to move from one internet service to another (e.g. from Hotmail to Gmail, Spotify to Deezer, Flickr to Picasa) and be able to take their information with them.

This right does not work well where there are no defined industry data formats to move such data from one provider to another (which is the case in most industries). But as a minimum, we need to be able to support clients that receive such requests from their users and a (documented) approach needs to be in place to enable such assistance. As with other rights, such a request would need to be reviewed by the Global Privacy Officer / Legal before any work starts.

Please also note the guidance on 4.2 which is applicable here as well.

A commonly available, structured and machine-readable format means a format which would allow the individual (or anyone else they give it to) reuse the data on their own machine, i.e. it should be interoperable. This would include a Word, Excel, XML, JSON or CSV file. It would not generally include a PDF file. This does not necessarily mean that all the information needs to be able to be extracted as one file, it can be provided as multiple files.

The information in scope is limited to Personal Information that:

- *(i) has been actively and knowingly provided by the individual or that has been "provided" by the user (user name or email address) or observed by Blackboard (e.g. activity logs) by virtue of the use of the system, and*
- *(ii) is processed by the client on the basis of the individual's consent or where processing by the client is necessary to perform a contract with the individual, falls into the scope of this requirement (this is an assessment that the client would need to undertake and that we would review as well).*

Inferred or derived data that has been created by the client or Blackboard is not in scope (e.g. student risk profile created by analysing provided or observed data, data created by algorithms used in the Client Product System).

A reasonable time period is likely to be 5 business days to ensure there is sufficient time for Global Privacy Officer/Legal to review the extracted data before it is provided to the client / user.

Requirement 5.2: Approach is in place and documented that allows to stop actively collecting / using information about a specific user where requested, so that no changes take place for that data (with the consequence that the user will no longer able to use the system) (e.g. through export/removal of data) (where Blackboard system is 'system of record').

Guidance: It must be possible to (temporarily) 'switch off' processing within a system or a system functionality (e.g. analytics) for a particular individual if the Client receives an objection or restriction request from an individual and asks Blackboard for assistance. This can be achieved by exporting the information and keeping it in a separate file / database where it is

no longer actively processed and then deleting the data in the live / production system. As with other requests, this needs to be reviewed / approved by the Global Privacy Officer / Legal before any work starts.

Such requests can only be fulfilled where the requested system or system functionality is not used anymore for the user.

A reasonable time period is likely to be 10 business days once reviewed / approved by Global Privacy Officer / Legal.

Blackboard Internal - Not to be shared externally