Blackboard

Blackboard Data Privacy Program Update

IMS Europe Summit October 2019

Stephan Geering, Global Privacy Officer

Blackboard’s Global Data Privacy Program

Data Privacy Program: Global GDPR baseline

Policies	Contracts	Processes	Governance	Client assurance
Global Data Privacy Policy	Client Data Processing Addendum	Privacy by design	Global Privacy Officer	Privacy Statement
Standards	Vendor Data Processing Addendum	Data Protection Impact Assessment	Data Privacy Champions	Privacy Center and Community
Product Requirements	Partner privacy clauses	Individual rights requests	Training and awareness	Privacy Shield certification
Vendor system requirements	User terms	Register of processing	Audits	(Binding Corporate Rules)*

* Submitted to Dutch Data Protection Authority 10 May 2019 – pending authorization

Global Data Privacy Program – Selected Areas

Client Data Processing Agreement

- Updating our client master agreement and DPA with aim to make it globally applicable
- Better reflect common negotiation positions
- Reduce negotiation friction and reduce percentage of negotiated DPAs

Binding Corporate Rules (BCRs)

- Strongest EU data transfer mechanism
- Submitted to Dutch Data Protection Authority for authorization 10 May 2019
- Evidence of strong data privacy program

DPIA

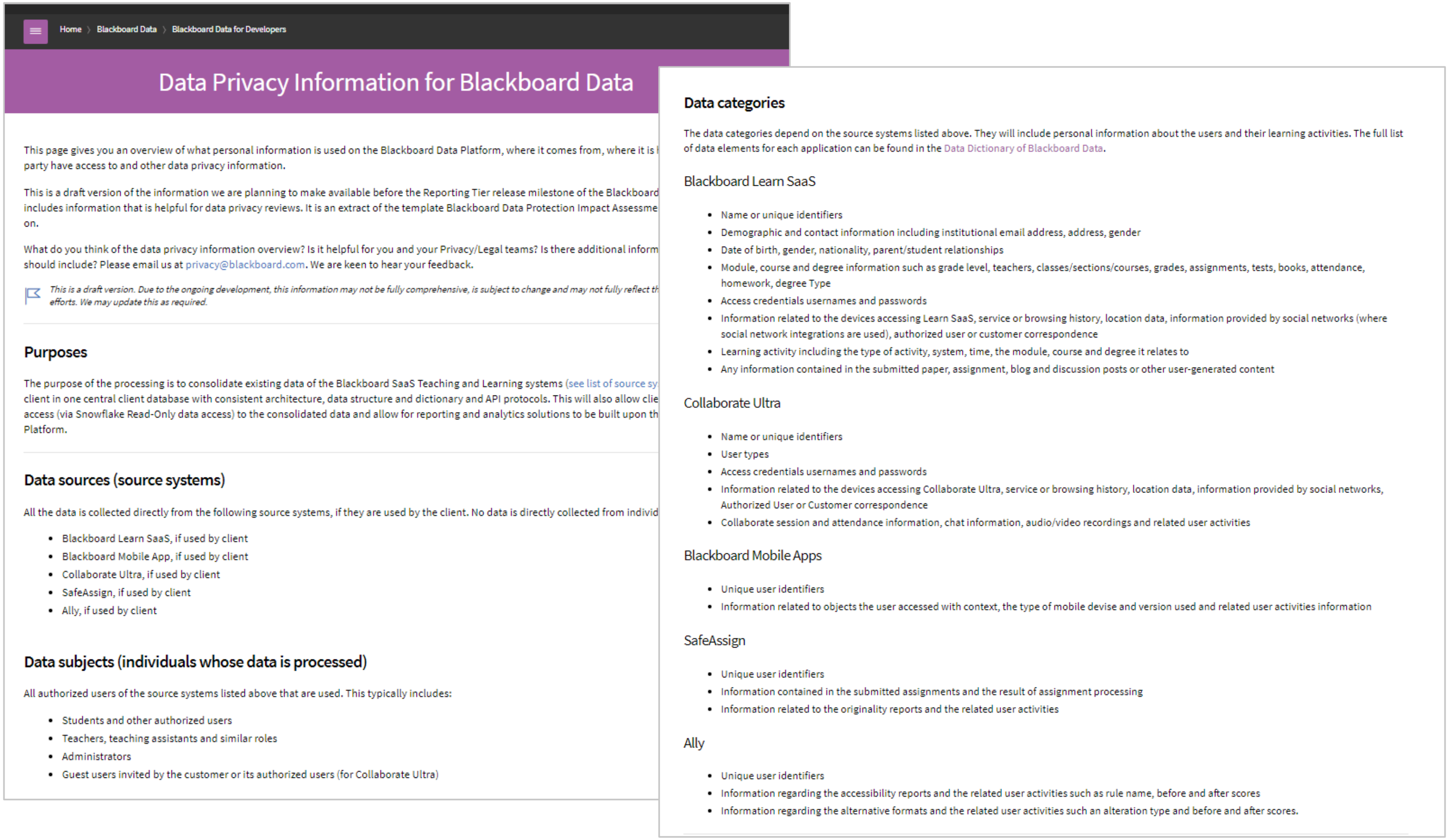
- DPIA for Blackboard Data platform in progress – will be available for clients
- Cross-functional working group including Privacy, Security, Product Management, Product Development and Architecture

Audit

- First audit under formal GDPR procedure in progress
- Risk-based, focused on key products and key areas of client/internal/regulatory concern
- Results reported to Compliance Committee

Enhanced product privacy information: Blackboard Data

https://help.blackboard.com/Blackboard_Data/Administrator/Personal_Information_in_Blackboard_Data



Data Privacy Information for Blackboard Data

This page gives you an overview of what personal information is used on the Blackboard Data Platform, where it comes from, where it is
party have access to and other data privacy information.

This is a draft version of the information we are planning to make available before the Reporting Tier release milestone of the Blackboard
includes information that is helpful for data privacy reviews. It is an extract of the template Blackboard Data Protection Impact Assessme
on.

What do you think of the data privacy information overview? Is it helpful for you and your Privacy/Legal teams? Is there additional inform
should include? Please email us at privacy@blackboard.com. We are keen to hear your feedback.

*This is a draft version. Due to the ongoing development, this information may not be fully comprehensive, is subject to change and may not fully reflect th
efforts. We may update this as required.*

Purposes

The purpose of the processing is to consolidate existing data of the Blackboard SaaS Teaching and Learning systems (see list of source sy
client in one central client database with consistent architecture, data structure and dictionary and API protocols. This will also allow clie
access (via Snowflake Read-Only data access) to the consolidated data and allow for reporting and analytics solutions to be built upon th
Platform.

Data sources (source systems)

All the data is collected directly from the following source systems, if they are used by the client. No data is directly collected from individ

- Blackboard Learn SaaS, if used by client
- Blackboard Mobile App, if used by client
- Collaborate Ultra, if used by client
- SafeAssign, if used by client
- Ally, if used by client

Data subjects (individuals whose data is processed)

All authorized users of the source systems listed above that are used. This typically includes:

- Students and other authorized users
- Teachers, teaching assistants and similar roles
- Administrators
- Guest users invited by the customer or its authorized users (for Collaborate Ultra)

Data categories

The data categories depend on the source systems listed above. They will include personal information about the users and their learning activities. The full list of data elements for each application can be found in the Data Dictionary of Blackboard Data.

Blackboard Learn SaaS

- Name or unique identifiers
- Demographic and contact information including institutional email address, address, gender
- Date of birth, gender, nationality, parent/student relationships
- Module, course and degree information such as grade level, teachers, classes/sections/courses, grades, assignments, tests, books, attendance, homework, degree Type
- Access credentials usernames and passwords
- Information related to the devices accessing Learn SaaS, service or browsing history, location data, information provided by social networks (where social network integrations are used), authorized user or customer correspondence
- Learning activity including the type of activity, system, time, the module, course and degree it relates to
- Any information contained in the submitted paper, assignment, blog and discussion posts or other user-generated content

Collaborate Ultra

- Name or unique identifiers
- User types
- Access credentials usernames and passwords
- Information related to the devices accessing Collaborate Ultra, service or browsing history, location data, information provided by social networks, Authorized User or Customer correspondence
- Collaborate session and attendance information, chat information, audio/video recordings and related user activities

Blackboard Mobile Apps

- Unique user identifiers
- Information related to objects the user accessed with context, the type of mobile devise and version used and related user activities information

SafeAssign

- Unique user identifiers
- Information contained in the submitted assignments and the result of assignment processing
- Information related to the originality reports and the related user activities

Ally

- Unique user identifiers
- Information regarding the accessibility reports and the related user activities such as rule name, before and after scores
- Information regarding the alternative formats and the related user activities such an alteration type and before and after scores.

Data privacy classification for EdTech platform*

Type	Description
Direct-identifier	Direct identifier such as name, user name, user ID, device ID, IP address, email address, and similar
Indirect identifier	Indirect identifier DOB, gender, postal address and similar data fields
Organizational identifier	Data fields that identify a specific organization such as client name, instance IDs
Government Identifier	SSN, passport numbers and similar government-issued identifiers
Obfuscated identifier	Direct/indirect identifiers that have been hashed or similarly obfuscated
Sensitive information	Race/ethnicity, health/genetic, religion, disability, union, criminal etc.
Biometric information	E.g. fingerprint, voice prints etc.
User activity	Internet, network or application activity information, that includes browsing history, search history, and information regarding the use of our products
User content	Files, assignments etc. uploaded/provided by user
Media file	Audio, video and similar media recordings content (e.g. Collab recording, video feedback)
Free form	Free form fields / data – likely to be considered PI
Device information	Information on the device of the user (e.g. device, ID, browser, OS information etc.)
Geolocation data	GPS, WiFi-based and other location (tracking) information
Purchasing/advertising history	If targeted advertising, information about ads that were displayed and clicked on etc. History of services purchased.
Payment/transaction data	Card payments, other financial transactions
Other financial data	Financial data E.g. financial aid data
Inferences data	Inferences drawn from any of the information to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

* Draft version – work in progress