

DATA PROCESSING AGREEMENT (DPA)

Between [REDACTED], below referred to as "**Controller**", and SMART Technologies ULC, below referred to as "**Processor**".

1. Background and purpose

1.1 According to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**"), it is required to have a written agreement between the Controller and the Processor that governs the processing of personal data that the Processor shall pursue on behalf of the Controller. In this case, the Controller is a Processor authorized reseller who will be providing the Processor (i.e., SMART) with point of sale (POS) customer purchase data.

1.2 This DPA between the Controller and the Processor ("**Parties**") regulates the outset obligations that the Processor shall have when processing personal data on behalf of the Controller. The purpose of this agreement is to ensure that the Processor processes personal data in accordance with the Controller's instruction and applicable law, which includes applicable law within EU/EEC, different regulations and decisions issued by authorities and recommendations from the European Data Protection Board that are applicable when processing personal data within the scope of the DPA.

1.3 The Processor in this DPA shall have its own relationship with its end users. No student data should be provided to Processor from the Controller.

PERSONUPPGIFTSBITRÄDESAVTAL

Mellan [REDACTED] (nedan "**Personuppgiftsansvarig**"), och SMART Technologies ULC, (nedan "**Personuppgiftsbiträdet**").

1. Bakgrund och syfte

1.1 Enligt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ("**Dataskyddsförordningen**") så är det nödvändigt att upprätta ett skriftligt avtal mellan den Personuppgiftsansvarige och ett Personuppgiftsbiträdet som reglerar behandlingen av personuppgifter som utförs av Personuppgiftsbiträdet för den Personuppgiftsansvariges räkning. I detta fall så är den Personuppgiftsansvarige en av Personuppgiftsbiträdet auktoriserad återförsäljare som kommer att tillhandahålla Personuppgiftsbiträdet (dvs. SMART) med uppgifter om kunders köp vid försäljningsstället.

1.2 Detta personuppgiftsbiträdesavtal ("**PuB-avtal**") mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet ("**Parterna**") reglerar de skyldigheter som Personuppgiftsbiträdet som utgångspunkt ska underställas när Personuppgiftsbiträdet behandlar personuppgifter för den Personuppgiftsansvariges räkning. Syftet med detta avtal är att säkerställa att Personuppgiftsbiträdet behandlar personuppgifter i enlighet med den Personuppgiftsansvariges instruktioner och tillämplig lag, vilket inkluderar tillämplig lag inom EU/EES, olika regler och beslut utfärdade av myndigheter samt rekommendationer från Europeiska dataskyddsstyrelsen som är tillämpliga på behandling av personuppgifter inom ramen för PuB-avtalet.

1.3 Personuppgiftsbiträdet ska ha en egen relation med sina slutanvändare. Den Personuppgiftsansvarige ska inte tillhandahålla Personuppgiftsbiträdet med uppgifter om studenter.

2 Definitions

- 2.1 The definitions set-out in this DPA shall have the corresponding definitions as stated in the GDPR and stated herein.

3. Processing of personal data

- 3.1 The Parties have entered into this DPA to govern the terms and conditions for the Processor's processing of personal data pursuant to the applicable Processor's Terms of Service and Privacy Policy ("TOSP") which should be pursued by the Processor on behalf of the Controller.
- 3.2 The Processor and persons that act on behalf of the Processor may process personal data only in accordance with the DPA and any additional written instructions that the Controller may provide from time to time.
- 3.3 The Processor shall only process personal data in order to fulfil their obligations according to the TOSP. If the Processor has not received instructions or is uncertain of the purpose of processing that is needed in order to perform a certain task that means or could mean processing of personal data, shall that Processor, without undue delay, inform the Controller about the matter and wait until further instructions are provided from the Controller.
- 3.4 The Processor shall at any given time follow the Processor's obligations according to applicable law and stay informed about such obligations regarding the processing of personal data according to the DPA. The Processor shall also at any given time follow the codes of conduct or certification that the Processor has committed to follow. The Processor shall at least, within the scope of this DPA, nominate an appropriate contact person for specific data protection issues.
- 3.5 The Processor commitments to follow applicable law, which shall, in all cases, be interpreted in relation to the nature of the Processor's services and typically means that the processor shall not in its sole discretion collect personal data or use personal data for any other purpose other than to fulfil the

2 Definitioner

- 2.1 De definitioner som används i detta PuB-avtal ska ha den innebörd som anges här och i Dataskyddsförordningen.

3. Behandling av personuppgifter

- 3.1 Parterna har ingått detta PuB-avtal för att reglera Personuppgiftsbitrådets behandling av personuppgifter mot bakgrund av Personuppgiftsbitrådets tillämpliga villkor och integritetspolicy ("Huvudavtalet") som ska efterlevas av Personuppgiftsbitrådet å Personuppgiftsansvarigs vägnar.
- 3.2 Personuppgiftsbitrådet och de som handlar för Personuppgiftsbitrådets räkning ska behandla personuppgifter enbart i enlighet med detta PuB-avtal samt andra ytterligare skriftliga instruktioner som den Personuppgiftsansvarige kan komma att ge från tid till annan.
- 3.3 Personuppgiftsbitrådet ska enbart behandla personuppgifter för att uppfylla sina åtaganden enligt Huvudavtalet. Om Personuppgiftsbitrådet inte har mottagit instruktioner eller är osäker på ändamålet med behandling som är nödvändig för att utföra en viss uppgift som inbegriper eller som kan inbegripa behandling av personuppgifter så ska Personuppgiftsbitrådet, utan onödigt dröjsmål, informera den Personuppgiftsansvarige om detta samt invänta instruktioner från den Personuppgiftsansvarige.
- 3.4 Personuppgiftsbitrådet ska efterleva den Personuppgiftsansvariges skyldigheter enligt tillämplig lag samt hålla sig informerad om sådana skyldigheter rörande behandlingen av personuppgifter enligt detta PuB-avtal. Personuppgiftsbitrådet ska även efterleva de uppförandekoder eller certifieringar som Personuppgiftsbitrådet har förbundit sig till att följa. Personuppgiftsbitrådet ska åtminstone, inom ramen för detta PuB-avtal, nominera en lämplig kontaktperson för vissa dataskyddsfrågor.
- 3.5 Personuppgiftsbitrådets åtaganden till att efterleva tillämplig lag, som i alla situationer ska tolkas i förhållande till typen av tjänster som Personuppgiftsbitrådet tillhandahåller och innebär typiskt sätt att personuppgiftsbitrådet inte efter eget omdöme ska samla in personuppgifter eller använda

agreed delivery according to the main reseller agreement. The Processor shall not, in any event, without an order from a relevant authority or mandatory law:

- a) collect or disclose personal data from or to any third party, if the Parties have not agreed anything else in writing,
- b) change the method for processing personal data that would increase the risk for the data subjects fundamental freedoms and rights,
- c) copy or recreate personal data for the Processor's sole use, or
- d) in any other way process personal data for purposes other than the ones that are stated in the Main TOSP and appurtenant appendices.

3.6 The Processor shall take all reasonable measures that are required according to article 32 in the GDPR. The additional measurements that should be taken into account are stated in the appended instructions from the Controller.

3.7 The Processor shall assist the Controller by taking suitable technical and organisational security measures, to the extent possible, to enable the Controller to perform its obligations as a Controller and its obligations in relation to requests regarding the exercise of the data subjects rights in accordance with Chapter III of the GDPR.

3.8 The Processor shall assist the Controller in ensuring that the obligations as stated in articles 33-36 in the GDPR can be fulfilled, taking into consideration the type of processing and the information that the Processor has access to.

4. Records of processing activities

4.1 The Processor or its representative shall maintain a record regarding all categories of processing activities carried out on behalf of the Controller. The record must contain, at a minimum, the following information:

personuppgifter för något annat ändamål än att fullgöra leverans i enlighet med det huvudsakliga återförsäljaravtalet. Personuppgiftsbiträdet ska inte under några omständigheter utan beslut från relevant myndighet eller om det inte krävs enligt tvingande lag:

- a) samla in eller lämna ut personuppgifter från eller till tredje part, om inte Parterna skriftligen har kommit överens om annat,
- b) ändra metoden för behandlingen av personuppgifter som skulle öka risken för de registrerades fri- och rättigheter,
- c) kopiera eller återskapa personuppgifter för Personuppgiftsbiträdet nyttjande för egen räkning, eller
- d) på något annat sätt behandla personuppgifter för andra ändamål än de som anges i Huvudavtalet med tillhörande bilagor.

3.6 Personuppgiftsbiträdet ska vidta samtliga rimliga åtgärder som krävs i enlighet med artikel 32 Dataskyddsförordningen. De ytterligare åtgärder som ska tas i beaktande anges i den bilagda instruktionen från den Personuppgiftsansvariga.

3.7 Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige genom att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder, i den mån det är möjligt, så att den Personuppgiftsansvarige kan fullgöra sina skyldigheter i egenskap av personuppgiftsansvarig och sina skyldigheter i förhållande till begäran om utövande av de registrerades rättigheter enligt kapitel III i Dataskyddsförordningen.

3.8 Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige med att se till att skyldigheterna enligt artikel 33-36 Dataskyddsförordningen kan fullgöras med beaktande av typen av behandling och den typ av information som Personuppgiftsbiträdet har tillgång till.

4. Register över personuppgiftsbehandling

4.1 Personuppgiftsbiträdet eller dess företrädare ska föra ett register över alla kategorier av behandling som Personuppgiftsbiträdet utför för den Personuppgiftsansvariges räkning.

Registret ska innehålla åtminstone följande information:

- | | |
|---|---|
| <p>a) name and contact details of the Processor or any retained sub-processor, for the Controller and for the Controller's or the Processor's representative and the data protection officer;</p> <p>b) the categories of processing which will be carried out on behalf of the Controller;</p> <p>c) the categories of recipients to whom the personal data has been, or will be, disclosed, including recipients in third countries or, where applicable, international organisations;</p> <p>d) documentation of suitable safeguards that have been taken, if any personal data is transferred to a third country that is not included in a decision which contains applicable provisions regarding an adequate security level or appropriate security measures, and</p> <p>e) where applicable, a general description of the technical and organisational security measures taken by the Processor according to applicable law.</p> <p>4.2 The Processor, shall make such records available to the Controller upon request or relevant supervisory authority containing the above content.</p> <p>4.3 If a data subject, upon the exercise of their rights, requests a record over the processing of their personal data, the Processor shall, after consultation with the Controller, upon request from the data subject or the Controller make such records available regarding such processing with the contents and in a way that is in line with applicable law.</p> <p>5. Confidentiality and security measures</p> <p>5.1 The Processor shall implement necessary technical and organisational safeguards in accordance with applicable law and thereby establish appropriate technical and</p> | <p>a) namn och kontaktuppgifter för Personuppgiftsbiträdet eller eventuella anlitade underbiträden, för den Personuppgiftsansvarige samt för den Personuppgiftsansvariges eller Personuppgiftsbitrådets företrädare och dataskyddsombudet,</p> <p>b) de kategorier av behandling som kommer att utföras för den Personuppgiftsansvariges räkning,</p> <p>c) de kategorier av mottagare till vilka personuppgifter har, eller kommer att, lämnas ut till, inklusive mottagare i tredje land eller, när det är tillämpligt, internationella organisationer,</p> <p>d) dokumentation av lämpliga skyddsåtgärder som har företagits i det fall personuppgifter överförs till tredje land som inte omfattas av ett beslut innehållande tillämpliga bestämmelser om adekvat skyddsnivå eller lämpliga skyddsåtgärder, samt</p> <p>e) om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits av Personuppgiftsbiträdet enligt tillämplig lag.</p> <p>4.2 Personuppgiftsbiträdet ska tillse att sådana register på begäran tillgängliggörs för den Personuppgiftsansvarige eller för relevant tillsynsmyndighet under ovan beskrivna förutsättningar.</p> <p>4.3 Om en registrerad vid utövandet av dennes rättigheter begär ut ett register över behandlingen av dess personuppgifter så ska Personuppgiftsbiträdet, efter att ha samrådit med den Personuppgiftsansvarige, vid mottagande av en begäran från den registrerade eller den Personuppgiftsansvarige tillhandahålla sådana register över sådan behandling med det innehåll och på sådant sätt som föreskrivs enligt tillämplig lag.</p> <p>5. Konfidentialitet och säkerhetsåtgärder</p> <p>5.1 Personuppgiftsbiträdet ska implementera nödvändiga tekniska och organisatoriska säkerhetsåtgärder i enlighet med tillämplig lag för att därmed kunna genomföra lämpliga</p> |
|---|---|

organisational measurements in order to protect personal data from unintentional or unlawful destruction, loss, or modification, from unauthorised disclosure, or from unauthorised access to the personal data which is transferred, stored, or otherwise processed mainly when the processing contains alignment or data over networks and/or any other unlawful processing. When assessing the appropriate security level, certain regards shall be taken to the risks that the processing results in, especially unintentional or unlawful destruction, loss, or modification, from unauthorised disclosure to personal data.

5.2 The Processor undertakes to process the personal data under strict confidentiality and will not disclose or make personal data accessible to any third party, if an approval has not been provided prior to this DPA or in any other way is required according to applicable law or for the execution of this DPA.

5.3 The Processor undertakes to secure that only relevant employees are allowed to gain access to the personal data the belongs to the Controller in order to fulfil the Processor's obligations under this DPA. The Processor shall ensure that the employees who are authorised to process personal data covered by this DPA are subject to confidentiality, either by law or an agreement, which should at least correspond to the confidentiality provisions in which are stipulated in this DPA. The Processor shall also ensure that the employees understand the meaning of the confidentially stipulated in this DPA. The confidentially that the Parties undertake in the DPA also applies during a period of time after this DPA has expired. However, it shall only apply to a period of time that is stated in applicable law.

5.4 The Processor may not without (i) the Controller's prior written consent, and (ii) after securing that such transfer is carried out in accordance with applicable law, transfer personal data outside of the EU/EEA or to a country that is not included in the list of exempted countries against such transfer according to applicable law. This prohibition is also subject to technical support, maintenance and similar services.

tekniska och organisatoriska åtgärder för att skydda personuppgifter från oavsiktlig eller otillåten förstöring, förlust eller ändring samt från obehörigt röjande eller obehörig åtkomst till personuppgifter som överförs, lagras eller på annat sätt behandlas, framförallt när behandling innebär justering eller uppgifter mellan nätverk och/eller annan otillåten behandling. Vid bedömningen av den lämpliga säkerhetsnivån ska viss hänsyn tas till den risk som behandlingen medför, särskilt oavsiktlig eller otillåten förstöring, förlust eller ändring eller obehörigt röjande av personuppgifter.

5.2 Personuppgiftsbiträdet åtar sig att behandla personuppgifter under strikt konfidentialitet och ska inte utlämna till eller tillgängliggöra personuppgifter för tredje part förutom i de fall godkännande har givits innan Parternas ingående av detta PuB-avtal eller på något annat sätt måste ges i enlighet med tillämplig lag eller för verkställandet av detta PuB-avtal.

5.3 Personuppgiftsbiträdet åtar sig att säkerställa att enbart relevanta anställda har tillgång till de personuppgifter som tillhör den Personuppgiftsansvarige för att fullgöra Personuppgiftsbiträdets åtaganden enligt detta PuB-avtal. Personuppgiftsbiträdet ska säkerställa att anställda som är behöriga att behandla personuppgifter inom ramen för detta PuB-avtal är bundna av sekretess genom lag eller avtal vilket minst ska motsvara de sekretessåtaganden som är angivna i detta PuB-avtal. Personuppgiftsbiträdet ska även tillse att de anställda är införstådda med sekretessåtagandena i detta PuB-avtal. De sekretessåtaganden som Parterna åtar sig enligt PuB-avtalet gäller även under viss tid efter det att detta PuB-avtal har slutat gälla, dock enbart under sådan period som anges i tillämplig lag.

5.4 Personuppgiftsbiträdet får inte utan (i) den Personuppgiftsansvariges föregående skriftliga medgivande och (ii) efter att ha säkerställt att sådan överföring utförs i enlighet med tillämplig lag överföra personuppgifter utanför EU/EES eller till ett land som inte ingår i den lista av länder som är undantagna från sådan överföring i enlighet med tillämplig lag. Detta förbud gäller även för teknisk support, underhåll och liknande tjänster.

6. Audit and request for information

- 6.1 The Processor shall without undue delay inform the Controller about potential contacts with relevant supervisory authority or any other authority regarding the processing of personal data. The Processor is not allowed to represent the Controller or in any way act on behalf of the Controller against relevant supervisory authority or any third party without a written consent from the Controller.
- 6.2 The Processor shall grant the Controller, or any third party mutually authorised by the Parties, access to all non-confidential information which is required and necessary to enable the Controller to verify and audit the Processor's compliance with the obligations that are stated in this DPA, the GDPR and any other regulation. The Processor shall also enable and assist in audits, including inspections, which are conducted by the Controller or by a third party authorised by the Controller.
- 6.3 The Processor is entitled to compensation from the Controller to compensate for reasonable direct cost that the Processor has suffered due to such audit or inspection.
- 6.4 The Processor shall grant the Controller access to all non-confidential information which is required and necessary to enable the Controller to verify compliance with the obligations that follow from this DPA and that the processing fulfils requirements according to applicable law.
- 6.5 In cases where a data subject, relevant supervisory authority or any other third party requests information from any of the Parties in respect of personal data, the Parties shall cooperate and exchange information in to the required extent.
- 6.6 The Processor may not disclose information where the Processor has not obtained a

6. Granskning och begäran om information

- 6.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål informera den Personuppgiftsansvarige om eventuell kontakt med en relevant tillsynsmyndighet eller andra myndigheter rörande behandlingen av personuppgifter. Personuppgiftsbiträdet får inte företräda den Personuppgiftsansvarige eller på något sätt agera handla för den Personuppgiftsansvariges räkning i förhållande till en relevant tillsynsmyndighet eller tredje part utan skriftligt medgivande från den Personuppgiftsansvarige.
- 6.2 Personuppgiftsbiträdet ska ge den Personuppgiftsansvarige, eller en av Parterna gemensamt utsedd behörig tredje part, tillgång till all icke-konfidentiell information som behövs och är nödvändig för att den Personuppgiftsansvarige ska kunna verifiera och granska Personuppgiftsbitrådets efterlevnad av de åtaganden som framgår av detta PuB-avtal, Dataskyddsförordningen och övriga lagar och regler. Personuppgiftsbiträdet ska även möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den Personuppgiftsansvarige eller tredje part som bemyndigats av den Personuppgiftsansvarige.
- 6.3 Personuppgiftsbiträdet har rätt till ersättning från den Personuppgiftsansvarige för rimliga direkta kostnader som Personuppgiftsbiträdet har drabbats av på grund av sådan granskning eller inspektion.
- 6.4 Personuppgiftsbiträdet ska ge den Personuppgiftsansvarige tillgång till all icke-konfidentiell information som behövs och som är nödvändig för att möjliggöra för den Personuppgiftsansvarige att verifiera efterlevnad med de skyldigheter som framgår av detta PuB-avtal och att behandlingen uppfyller de krav som ställs enligt tillämplig lag.
- 6.5 Om en registrerad, relevant tillsynsmyndighet eller annan tredje part begär information från någon av Parterna gällande personuppgifter så ska Parterna samarbeta och utbyta information i sådan utsträckning som är nödvändig.
- 6.6 Personuppgiftsbiträdet får inte lämna ut information om det inte följer av en skyldighet

written consent from the Controller to do so, or, other than if such obligation is mandatory according to applicable law or an order from any relevant authority.

7. Sub-processors

7.1 The Processor may not retain sub-processors to process personal data on behalf of the Controller without informing the Controller in written form that the Processor will retain a sub-processor thirty (30) days prior to such engagement.

7.2 In the event that the Processor retains a sub-processor for the processing of personal data, the Processor shall impose the same undertakings and obligations which follow this DPA. The Processor shall also undertake to make sure that the sub-processor respects and follows the terms that are applicable under this Data Processor TOSP and otherwise follow by applicable law.

7.3 In the event that the Processor in accordance with this DPA, retains a sub-processor, the Processor shall ensure that the agreement between the Processor and the sub-processor is construed in such way that the sub-processor is also bound by this DPA as well as the requirements stated in this agreement and applicable law. In the event the sub-processor fails to fulfil its obligations, the Processor shall bear full liability towards the Controller for the performance of such sub-processor's obligations. The Processor shall, from time to time, maintain an updated list of the sub-processors who may be retained. At the Controller's request, the Processor shall submit a copy of the list to the Controller.

7.4 The Controller, or any party authorised by the Controller, has the right to be assisted by the Processor when conducting an inspection or audit regarding the processing of personal data that is performed by the retained sub-processor.

8. Personal data breach

8.1 In the event that the Processor suspects or detects any type of security breach such as unauthorised access, destruction, change to personal data or anything, or if the Processor for any reason cannot fulfil the undertakings and obligations in this DPA, shall the

i tvingande lag eller föreläggande från en relevant myndighet eller annars utan den Personuppgiftsansvariges skriftliga samtycke.

7. Underbiträden

7.1 Personuppgiftsbiträdet ska skriftligen och med trettio (30) dagars varsel informera den Personuppgiftsansvarige innan Personuppgiftsbiträdet avser att anlita ett underbiträde för att behandla personuppgifter för den Personuppgiftsansvariges räkning.

7.2 Om Personuppgiftsbiträdet anlitar ett underbiträde för att behandla personuppgifter så ska Personuppgiftsbiträdet tillse att underbiträdet är bundet av minst de åtaganden och skyldigheter som följer av detta PuB-avtal. Personuppgiftsbiträdet ska även tillse att underbiträdet efterlever de villkor som gäller enligt Huvudavtalet samt i övrigt vad som följer av tillämplig lag.

7.3 I det fall att Personuppgiftsbiträdet anlitar ett underbiträde i enlighet med detta PuB-avtal ska Personuppgiftsbiträdet säkerställa att underbiträdet genom avtalet mellan Personuppgiftsbiträdet och underbiträdet blir bunden av detta PuB-avtal samt de krav som framgår av detta avtal och tillämplig lag. Om underbiträdet inte fullgör sina skyldigheter ska Personuppgiftsbiträdet vara fullt ansvarig gentemot den Personuppgiftsansvarige för utförandet av underbiträdets skyldigheter. Personuppgiftsbiträdet ska från tid till annan föra en uppdaterad lista med de underbiträden som kan komma att anlitas. Personuppgiftsbiträdet ska vid förfrågan skicka en kopia av listan till den Personuppgiftsansvarige.

7.4 Den Personuppgiftsansvarige, eller annan av Personuppgiftsansvarig utsedd tredje part, har rätt att begära att Personuppgiftsbiträdet ska bidra till utförandet av en inspektion eller granskning av behandlingen av personuppgifter som utförs av ett anlitat underbiträde.

8. Personuppgiftsincident

8.1 Om Personuppgiftsbiträdet misstänker eller upptäcker någon form av säkerhetsincident, såsom obehörig tillgång till, eller förstöring eller ändring av, personuppgifter eller annat, eller i det fall Personuppgiftsbiträdet av någon anledning inte kan fullgöra sina åtaganden

Processor immediately investigate the incident and take appropriate measures in order to mend the incident and prevent any recurrence of such events.

och skyldigheter i enlighet med detta PuB-avtal så ska Personuppgiftsbiträdet omedelbart undersöka incidenten och vidta lämpliga åtgärder för att åtgärda incidenten samt förhindra att sådan händelse upprepas.

8.2 The Processor shall without undue delay notify the Controller, after the Processor has learned of a personal data breach and shall after this breach provide the Controller with on-going information about the breach as information about the breach becomes accessible to the Processor. The notification shall at least contain the following:

- a) a description of the nature of the personal data breach, if possible, the categories and approximate number of affected data subjects, and the categories and approximate numbers of affected personal data records;
- b) provide the name of and the contact information to the data protection officer or other contact points where more information can be found,
- c) description of the likely consequences of the personal data breach, and
- d) a description of the measures that the Processor has taken or proposed in order to remediate the breach, comprised of, when appropriate, measurements in order to mitigate the potential negative effects.

8.3 The Processor shall immediately inform the Controller if;

- a) the Processor retains knowledge of processing of personal data that contradicts the Controller's instruction or this DPA, and/or
- b) the Processor considers that an instruction contradicts applicable law.

8.4 If a certain type of processing, especially in regard to the use of new technology and considering the type, extent, context and purpose, may probably lead to a high risk for physical persons rights and freedoms shall the Processor, before the processing is performed, assist the Controller in the assessment of the planned processed consequences for the protection of personal data.

8.2 Personuppgiftsbiträdet ska utan onödigt dröjsmål meddela den Personuppgiftsansvarige efter det att Personuppgiftsbiträdet har fått kännedom om en personuppgiftsincident och ska ge den Personuppgiftsansvarige löpande information rörande incidenten i takt med att information blir tillgänglig för Personuppgiftsbiträdet. Sådant meddelande ska åtminstone:

- a) beskriva personuppgiftsincidentens art inbegripet, om möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
- b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
- c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
- d) beskriva de åtgärder som Personuppgiftsbiträdet har vidtagit eller föreslagit för att åtgärda incidenten, inbegripet, när det är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

8.3 Personuppgiftsbiträdet ska omedelbart informera den Personuppgiftsansvarige om:

- a) Personuppgiftsbiträdet får vetskap om personuppgiftsbehandling som står i strid med den Personuppgiftsansvariges instruktioner eller detta PuB-avtal och/eller,
- b) Personuppgiftsbiträdet anser att en instruktion skulle stå i strid med tillämplig lag.

8.4 Om en viss typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, troligtvis kan komma att leda till en hög risk för fysiska personers fri- och rättigheter så ska Personuppgiftsbiträdet, innan behandlingen utförs, bistå den Personuppgiftsansvarige med vederbörandes bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

9. Liability

- 9.1 Article 82 of the GDPR shall apply in case of damages awarded to a data subject, through a court decision or other decision, due to a breach of any provision in this DPA, instruction from the Controller or applicable data protection regulations.
- 9.2 When an administrative fine is imposed according to article 83 of GDPR or 6 chap. 2 § of the Act containing supplementary provisions to the EU General Data Protection Regulation (2018:218), the administrative fine shall be paid by the Party receiving such fine.
- 9.3 If either Party receives knowledge of a circumstance that can lead to a loss for the other party, that Party shall immediately inform the other party of the circumstances and actively work together with the other party in order to prevent and minimise such loss.
- 9.4 Despite what has been stated in the Parties TOSP and related appendices, sections 9.1 and 9.2 in the DPA shall apply before any other regulations regarding the parties cessation of obligation between them covering the processing of personal data.

10. Compensation

- 10.1 The Processor is not entitled to any compensation for measures which the Processor takes in respect of processing of personal data, besides otherwise stated in this DPA or the Parties reseller agreement.

11. Effective term

- 11.1 This DPA enters into force on the day which it is signed and applies as long as the Processor processes personal data under the Parties TOSP.

12 Termination

- 12.1 When the Processor discontinues processing personal data on behalf of the Controller under this DPA, the Processor shall at the choice of the Controller destroy, erase and/or

9. Ansvar

- 9.1 Artikel 82 Dataskyddsförordningen ska gälla avseende ersättning som utdömts till registrerad genom domstolsbeslut eller annat beslut på grund av överträdelse av en bestämmelse i detta PuB-avtal, av instruktion från den Personuppgiftsansvarige eller tillämplig dataskyddslagstiftning.
- 9.2 När en administrativ sanktionsavgift utfärdas i enlighet med artikel 83 Dataskyddsförordningen eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska den administrativa sanktionsavgiften betalas av den Part som sanktionsavgiften riktas till.
- 9.3 Om endera Part blir får kännedom en omständighet som kan leda till en förlust för den andra Parten så ska Parten omedelbart informera den andra Parten om omständigheterna och aktivt arbeta tillsammans för att förebygga och minimera sådan förlust.
- 9.4 Oavsett vad som har angetts i Parternas Huvudavtal samt tillhörande bilagor, ska punkterna 9.1 och 9.2 i PuB-avtalet ha företräde framför andra bestämmelser angående upphörande av skyldigheter mellan parterna angående behandlingen av personuppgifter.

10. Ersättning

- 10.1 Personuppgiftsbiträdet är inte berättigat till ersättning för åtgärder som Personuppgiftsbiträdet vidtar avseende behandlingen av personuppgifter, om inte annat angetts i detta Biträdeavtal eller i Parternas återförsäljaravtal.

11. Avtalets löptid

- 11.1 Detta PuB-avtal börjar gälla den dag det undertecknas och gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter enligt Partneras Huvudavtal.

12 Avtalets upphörande

- 12.1 När Personuppgiftsbiträdet upphör med behandling av personuppgifter för den Personuppgiftsansvariges räkning enligt detta PuB-avtal så ska Personuppgiftsbiträdet

return all personal data which is associated with this agreement to the Controller in accordance with the Controller's instruction and ensure that no personal data or copies of personal data are still in the Processor's possession unless required by applicable law or financial reasons, including tax.

- 12.2 The Processor shall once this DPA is terminated, ensure that the obligation stated in section 12.1 of the DPA also applies to any sub-processor.

13. Amendments

- 13.1 The Controller may due to necessary compliance with applicable law, amend the contents of this this DPA. An amendment may enter into force thirty (30) days after the Controller has sent a notice to the Processor regarding the amendment. In the event that the Processor does not accept the relevant amendment, the Controller shall have the right to terminate all agreements with the Processor under which the Processor shall process personal data.

- 13.2 Amendments to this DPA shall be made in writing and signed by both Parties in order to legally binding.

14. Standard contractual clauses

- 14.1 Within the scope of the COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council the standard contractual clauses ("SCC") attached in Annex 1 shall apply.

15. Applicable provisions and order of precedence

- 15.1 The agreements between the parties apply in the following order, whereby, in case of contradictions, provisions of the documents first mentioned shall prevail over the provisions in the documents mentioned thereafter:

- a) SCC subject to this DPA in Annex 1;

förstöra, radera och/eller återlämna alla personuppgifter, beroende på vad den Personuppgiftsansvarige väljer, som är hänförliga till detta PuB-avtal i enlighet med den Personuppgiftsansvariges instruktioner samt säkerställa att inga personuppgifter eller kopior av personuppgifter fortsatt är i Personuppgiftsbitrådets besittning, såvida inte lagring av personuppgifterna krävs enligt tillämplig lag eller av finansiella- eller skatteskäl.

- 12.2 Personuppgiftsbitrådet ska vid PuB-avtalets upphörande säkerställa att de åtaganden som framgår av punkt 12.1 även gäller för eventuella underbiträden.

13. Ändringar

- 13.1 Den Personuppgiftsansvarige kan komma att ändra innehållet i detta PuB-avtal om det är nödvändigt för att efterleva tillämpliga lag. Ändringar börjar gälla trettio (30) dagar efter att den Personuppgiftsansvarige meddelat Personuppgiftsbitrådet om ändringen. I det fall att Personuppgiftsbitrådet inte accepterar ändringen så har den Personuppgiftsansvarige rätt att säga upp alla avtal med Personuppgiftsbitrådet inom ramen för vilka Personuppgiftsbitrådet ska behandla personuppgifter.

- 13.2 Ändringar av detta PuB-avtal ska göras skriftligen och ska undertecknas av bägge Parter för att vara bindande.

14. Standaravtalsklausuler

Inom ramen för Kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 så ska standardavtalsklausulerna ("SCC") i Bilaga 1 gälla.

15. Tillämpliga bestämmelser och prioritet

- 15.1 Vid eventuella motstridigheter i avtalen mellan Parterna ska avtalen äga tillämpning enligt följande ordningsföljd:

- a) SCC i detta PuB-avtal enligt Bilaga 1,

- b) the provisions of this DPA and
- c) the provisions of the TOSP.

16. **Governing law and jurisdiction**

16.1 This DPA shall be governed by the substantive law of [REDACTED]. Any dispute, controversy or claim arising out of or in connection with this DPA, shall be finally settled in the general courts of [REDACTED] with the district court of [REDACTED] as the first instance.

This DPA may be executed, including electronically, in any number of counterparts.

Date

Date

Controller

Processor

Name & Title

Name & Title

- b) Bestämmelserna i detta PuB-avtal, och
- c) Bestämmelserna i Huvudavtalet.

16. **Tillämplig lag och tillämpligt forum**

16.1 [REDACTED] lag ska tillämpas på detta PuB-avtal. Tvist som uppstår i anledning av PuB-avtalet ska slutligt avgöras i [REDACTED] domstol, med [REDACTED] tingsrätt som första instans.

Detta PuB-avtal kan komma att undertecknas i ett eller flera original exemplar (till exempel digitalt)

Datum

Datum

Ansvarig

Biträde

Namn & befattning

Namn & befattning

ANNEX 1: STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor

BILAGA 1: STANDARDAVTALSKLAUSULER

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

1. Clause 1 – Purpose and scope	1. Klausul 1 - Syfte och tillämpningsområde
1.1 The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ¹ for the transfer of data to a third country.	1.1 Syftet med dessa standardavtalsklausuler är att säkerställa överensstämmelse med kraven i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning) ¹ vid överföring av personuppgifter till ett tredjeland.
1.2 The Parties	1.2 Parterna
1.2.1 the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and	1.2.1 den eller de fysiska eller juridiska personer, den eller de offentliga myndigheter, den eller de byråer eller andra organ (enheterna) som överför personuppgifter enligt förteckningen i bilaga I.A. (uppgiftsutföraren), och
1.2.2 the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').	1.2.2 den eller de enheter i ett tredjeland som tar emot personuppgifter från uppgiftsutföraren, direkt eller indirekt via en annan enhet som också är part i dessa klausuler, enligt förteckningen i bilaga I.A. (uppgiftsinföraren)
1.3 These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.	1.3 Dessa klausuler är tillämpliga med avseende på överföring av personuppgifter enligt vad som anges i bilaga I.B.
1.4 The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.	1.4 Det tillägg till dessa klausuler som innehåller de bilagor som det hänvisas till utgör en integrerad del av dessa klausuler.
2. Clause 2 – Effect and invariability of the Clauses	2. Klausul 2 – Klausulernas verkan och beständighet
2.1 These Clauses set out appropriate safeguards, including	2.1 Genom dessa klausuler fastställs lämpliga skyddsåtgärder, däribland

	enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.		verkställbara rättigheter och effektiva rättsmedel för de registrerade enligt artikel 46.1 och artikel 46.2 c i förordning (EU) 2016/679 och, när det gäller överföring av personuppgifter från personuppgiftsansvariga till personuppgiftsbiträden och/eller från personuppgiftsbiträden till personuppgiftsbiträden, standardavtalsklausuler enligt artikel 28.7 i förordning (EU) 2016/679, under förutsättning att de inte ändras, förutom för att välja en eller flera lämpliga moduler eller lägga till eller uppdatera informationen i tillägget. Detta hindrar inte parterna från att inbegripa de standardavtalsklausuler som fastställs i dessa klausuler i ett mer övergripande avtal och/eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med dessa klausuler eller påverkar de registrerades grundläggande rättigheter eller friheter.
2.2	These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.	2.2	Dessa klausuler påverkar inte de skyldigheter som uppgiftsutföraren omfattas av med stöd av förordning (EU) 2016/679.
3.	Clause 3 – Third-party beneficiaries	3.	Klausul 3 – Berättigade tredje parter
3.1	Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:	3.1	Registrerade personer får åberopa och verkställa dessa klausuler, i egenskap av berättigade tredje parter, gentemot uppgiftsutföraren och/eller uppgiftsinföraren, med följande undantag:
3.2	Clause 1, Clause 2, Clause 3, Clause 6; Clause 7;	3.2	Klausul 1, klausul 2, klausul 3, klausul 6, klausul 7.
3.3	Clause 8.1.2, 8.9.1, 8.9.3, 8.9.4 and 8.9.5;	3.3	Klausul 8 – modul ett: klausul 8.5 e och klausul 8.9 b; modul två: klausul 8.1 b, 8.9 a, c, d och e; modul tre: klausul 8.1 a, c och d och klausul 8.9 a, c, d, e, f och g; modul fyra: klausul 8.1 b och klausul 8.3 b.
3.4	Clause 9.1, 9.3, 9.4 and 9.5;	3.4	Klausul 9 – modul två: klausul 9 a, c, d och e; modul tre: klausul 9 a, c, d och e.
3.5	Clause 12.1, 12.4 and 12.6;	3.5	Klausul 12 – modul ett: klausul 12 a och d; modulerna två och tre: klausul 12 a, d och f.

3.6	Clause 13;	3.6	Klausul 13.
3.7	Clause 15.1.3, 15.1.4 and 15.1.5;	3.7	Klausul 15.1 c, d och e.
3.8	Clause 16.5;	3.8	Klausul 16 e.
3.9	Clause 18.1 and 18.2.	3.9	Klausul 18 – modulerna ett, två och tre: klausul 18 a och b; modul fyra: klausul 18.
3.10	Paragraph 3.1 is without prejudice to rights of data subjects under Regulation (EU) 2016/679.	3.10	Led 3.1 påverkar inte de registrerades rättigheter enligt förordning (EU) 2016/679.
4.	Clause 4 - Interpretation	4.	Klausul 4 – Tolkning
4.1	Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.	4.1	Om begrepp som definieras i förordning (EU) 2016/679 används i dessa klausuler ska begreppen ha samma betydelse som i den förordningen.
4.2	These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.	4.2	Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.
4.3	These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.	4.3	Dessa klausuler ska inte tolkas på ett sätt som står i strid med de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679.
5.	Clause 5 – Hierarchy	5.	Klausul 5 - Hierarki
	In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.		Om en konflikt uppstår mellan dessa klausuler och bestämmelserna i de överenskommelser mellan parterna som gäller vid den tidpunkt då dessa klausuler överenskoms eller därefter träder i kraft, ska dessa klausuler ha företräde.
6.	Clause 6 – Description of the transfer(s)	6.	Klausul 6 – Beskrivning av överföringen eller överföringarna
	The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.		Närmare uppgifter om överföringen eller överföringarna, och i synnerhet de kategorier av personuppgifter som överförs och det eller de ändamål för vilka de överförs, anges i bilaga I.B.
7.	Clause 7 – Docking clause	7.	Klausul 7 – Dockningsklausul

7.1	[Intentionally deleted]	7.1	[Medvetet borttagen]
	SECTION II – OBLIGATIONS OF THE THIRD PARTIES		AVSNITT II – PARTERNAS SKYLDIGHETER
8.	Clause 8 – Data protection safeguards	8.	Klausul 8 – Skyddsåtgärder för uppgifter
	The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.		Uppgiftsutföraren garanterar att han eller hon har gjort rimliga ansträngningar för att se till att uppgiftsinföraren, genom genomförandet av lämpliga tekniska och organisatoriska åtgärder, kan fullgöra sina skyldigheter enligt dessa klausuler.
8.1	Instructions	8.1	Instruktioner
8.1.1	The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.	8.1.1	Uppgiftsinföraren ska endast behandla personuppgifterna enligt dokumenterade instruktioner från uppgiftsutföraren. Uppgiftsutföraren får ge sådana instruktioner under hela avtalets giltighetstid.
8.1.2	The data importer shall immediately inform the data exporter if it is unable to follow those instructions.	8.1.2	Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren om han eller hon inte kan följa dessa instruktioner.
8.2	Purpose limitations	8.2	Ändamålsbegränsning
	The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.		Uppgiftsinföraren ska endast behandla personuppgifterna för det eller de specifika ändamålen med överföringen, enligt vad som fastställs i bilaga I.B, såvida inte uppgiftsutföraren har gett andra instruktioner.
8.3	Transparency	8.3	Öppenhet
	On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful		På begäran ska uppgiftsutföraren tillhandahålla en kopia av dessa klausuler, inklusive tillägget när det har fyllts i av parterna, till den registrerade utan kostnad. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive de åtgärder som beskrivs i bilaga II och personuppgifter, får uppgiftsutföraren redigera delar av texten i tillägget till dessa klausuler innan en kopia tillhandahålls, men han eller hon måste bifoga en meningsfull sammanfattning om den registrerade annars inte skulle

summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

kunna förstå dess innehåll eller utöva sina rättigheter. På begäran ska parterna tillhandahålla skälen till redigeringen till den registrerade, i möjligaste mån utan att avslöja de redigerade uppgifterna. Denna klausul påverkar inte uppgiftsutförarens skyldigheter enligt artiklarna 13 och 14 i förordning (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.4 Korrekthet

Om uppgiftsinföraren får kännedom om att de personuppgifter som han eller hon har tagit emot är felaktiga, eller har blivit inaktuella, ska han eller hon informera uppgiftsutföraren utan onödigt dröjsmål. I sådana fall ska uppgiftsinföraren samarbeta med uppgiftsutföraren för att radera eller rätta uppgifterna.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14.5 to notify the

8.5 Behandlingens varaktighet och radering eller återlämnande av uppgifter

Uppgiftsinförarens behandling ska endast äga rum under den period som anges i bilaga I.B. När tillhandahållandet av behandlingstjänsterna har avslutats ska uppgiftsinföraren, enligt uppgiftsutförarens val, radera alla personuppgifter som behandlats på uppdrag av uppgiftsutföraren och intyga för uppgiftsutföraren att detta har skett, eller till uppgiftsutföraren återlämna alla personuppgifter som har behandlats på uppdrag av uppgiftsutföraren och radera befintliga kopior. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen. Detta påverkar inte klausul 14, i synnerhet kravet enligt klausul 14.5 att uppgiftsinföraren under hela avtalets giltighetstid ska meddela

data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14.1.

uppgiftsutföraren om han eller hon har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i klausul 14.1.

8.6 Security of processing

8.6 Säkerhet vid behandling

8.6.1 The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.1 Uppgiftsinföraren, och under överföring även uppgiftsutföraren, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa uppgifternas säkerhet, däribland genom skydd mot säkerhetsbrott som skulle leda till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande eller obehörig åtkomst till uppgifterna (personuppgiftsincident). Vid bedömning av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till de senaste rönen, kostnaderna för genomförandet, behandlingens karaktär, omfattning, sammanhang och ändamål samt riskerna för de registrerade i samband med behandlingen. Parterna ska i synnerhet överväga att använda kryptering eller pseudonymisering, även under överföringen, om ändamålet med behandlingen kan uppfyllas på detta sätt. Vid användning av pseudonymisering ska uppgiftsutföraren om möjligt behålla sin fullständiga kontroll över den ytterligare information som krävs för att knyta personuppgifterna till en viss registrerad. För att fullgöra sina skyldigheter enligt denna punkt ska uppgiftsinföraren åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga II. Uppgiftsinföraren ska göra regelbundna kontroller för att säkerställa att dessa åtgärder även fortsättningsvis ger en lämplig säkerhetsnivå.

8.6.2 The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management

8.6.2 Uppgiftsinföraren ska endast ge sin personal tillgång till personuppgifterna i den utsträckning det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Uppgiftsinföraren

	and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.		ska säkerställa att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iakttäta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
8.6.3	In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.	8.6.3	I händelse av en personuppgiftsincident som gäller uppgifter som har behandlats av uppgiftsföraren enligt dessa klausuler ska uppgiftsföraren vidta lämpliga åtgärder för att hantera incidenten, däribland åtgärder för att mildra dess negativa konsekvenser. Uppgiftsföraren ska även meddela uppgiftsutföraren utan onödigt dröjsmål efter att ha fått kännedom om incidenten. Meddelandet ska innehålla uppgifter om en kontaktpunkt som kan lämna mer information, en beskrivning av incidentens karaktär (inbegripet, om möjligt, vilka kategorier och det ungefärliga antalet registrerade och personuppgiftsregister som berörs), dess sannolika konsekvenser samt vilka åtgärder som har vidtagits eller föreslagits för att hantera incidenten, däribland, i tillämpliga fall, åtgärder för att mildra dess möjliga negativa konsekvenser. Om, och i den mån, det inte är möjligt att tillhandahålla all information vid samma tillfälle ska det inledande meddelandet innehålla den information som då finns tillgänglig, varefter ytterligare information ska tillhandahållas utan onödigt dröjsmål efterhand som den blir tillgänglig.
8.6.4	The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.	8.6.4	Uppgiftsföraren ska samarbeta med och bistå uppgiftsutföraren så att uppgiftsutföraren kan fullgöra sina skyldigheter enligt förordning (EU) 2016/679, framför allt att meddela den behöriga tillsynsmyndigheten och de berörda registrerade, med beaktande av behandlingens karaktär och den information som finns tillgänglig för uppgiftsföraren.
8.7	Sensitive data	8.7	Känsliga uppgifter

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

Om överföringen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar och lagöverträdelser (känsliga uppgifter) ska uppgiftsinföraren tillämpa de särskilda begränsningar och/eller de ytterligare skyddsåtgärder som beskrivs i bilaga I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union² (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- 8.8.1 the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- 8.8.2 the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- 8.8.3 the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- 8.8.4 the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

8.8 Vidare överföringar

Uppgiftsinföraren ska endast lämna ut personuppgifter till en tredje part enligt dokumenterade instruktioner från uppgiftsutföraren. Dessutom får uppgifterna endast lämnas ut till en tredje part utanför Europeiska unionen² (i samma land som uppgiftsinföraren eller i ett annat tredjeland, nedan kallat vidare överföring), om den tredje parten är eller samtycker till att vara bunden av dessa klausuler i motsvarande modul, eller

- 8.8.1 om den vidare överföringen sker till ett land som omfattas av ett beslut om adekvat skyddsnivå enligt artikel 45 i förordning (EU) 2016/679 som täcker den vidare överföringen,
- 8.8.2 om den tredje parten på annat sätt säkerställer lämpliga skyddsåtgärder enligt artikel 46 eller 47 i förordning (EU) 2016/679 med avseende på behandlingen i fråga,
- 8.8.3 om den vidare överföringen är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk i samband med särskilda administrativa, tillsynsrelaterade eller rättsliga förfaranden, eller
- 8.8.4 om den vidare överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den

			registrerade eller för en annan fysisk person.
	Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.		Vid varje vidare överföring måste uppgiftsinföraren uppfylla kraven för alla andra skyddsåtgärder i dessa klausuler, i synnerhet ändamålsbegränsning.
8.9	Documentation and compliance	8.9	Dokumentation och efterlevnad
8.9.1	The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.	8.9.1	Uppgiftsinföraren ska skyndsamt och på ett lämpligt sätt hantera förfrågningar från uppgiftsutföraren angående behandlingen enligt dessa klausuler.
8.9.2	The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.	8.9.2	Parterna ska kunna visa att de uppfyller kraven i dessa klausuler. Framför allt ska uppgiftsinföraren föra lämplig dokumentation över den behandling som utförts på uppdrag av uppgiftsutföraren.
8.9.3	The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.	8.9.3	Uppgiftsinföraren ska se till att uppgiftsutföraren har tillgång till all information som behövs för att visa att de skyldigheter som fastställs i dessa klausuler har fullgjorts och, på uppgiftsutförarens begäran, möjliggöra och bidra till revisioner av den behandling som omfattas av dessa klausuler med rimliga mellanrum eller om det finns indikationer på bristande efterlevnad. När beslut fattas om en granskning eller revision får uppgiftsutföraren ta hänsyn till relevanta intyg som innehas av uppgiftsinföraren.
8.9.4	The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.	8.9.4	Uppgiftsutföraren får välja att utföra revisionen själv eller anlita en oberoende revisor. Revisionerna får omfatta inspektioner i uppgiftsinförarens lokaler eller fysiska anläggningar och ska, om så är lämpligt, utföras med rimligt varsel.
8.9.5	The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.	8.9.5	Parterna ska se till att den information som avses i leden 8.9.2 och 8.9.3, inklusive resultaten av eventuella revisioner, finns tillgänglig för den behöriga tillsynsmyndigheten på begäran

9. Clause 9 – Use of sub-processors

9.1 GENERAL WRITTEN AUTHORISATION - The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9. Klausul 9 – Användning av underentreprenörer

9.1 ALLMÄNT SKRIFTLIGT TILLSTÅND
Uppgiftsinföraren har uppgiftsutförarens allmänna tillstånd att anlita en eller flera underentreprenörer i en överenskommen förteckning. Uppgiftsinföraren ska informera uppgiftsutföraren skriftligen om alla planerade ändringar av förteckningen genom tillägg eller ersättning av underentreprenörer minst [ange tidsperiod] i förväg, så att uppgiftsutföraren har tillräckligt med tid för att invända mot sådana ändringar före anlitandet av underentreprenören(-erna). Uppgiftsinföraren ska ge uppgiftsutföraren all information som behövs för att uppgiftsutföraren ska kunna utöva sin rätt att göra invändningar.

9.2 Om uppgiftsinföraren anlitar en underentreprenör för att utföra särskilda behandlingar (på uppdrag av uppgiftsutföraren) ska han eller hon göra detta genom ett skriftligt avtal som, i sak, innehåller samma skyldigheter i fråga om dataskydd som de avtal som är bindande för uppgiftsinföraren enligt dessa klausuler, däribland vad gäller de registrerades rättigheter som berättigade tredje parter. Parterna är överens om att uppgiftsinföraren, genom att uppfylla kraven i denna klausul, fullgör sina skyldigheter enligt klausul 8.8. Uppgiftsinföraren ska säkerställa att underentreprenören fullgör de skyldigheter som uppgiftsinföraren omfattas av enligt dessa klausuler.

9.3 Uppgiftsinföraren ska, på uppgiftsutförarens begäran, tillhandahålla en kopia av avtalet med underentreprenören och eventuella senare ändringar till uppgiftsutföraren. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsinföraren redigera texten i avtalet innan en kopia tillhandahålls.

9.4	The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.	9.4	Uppgiftsföraren ska fortsatt vara fullt ansvarig inför uppgiftsföraren för fullgörandet av underentreprenörens skyldigheter inom ramen för dennes avtal med uppgiftsföraren. Uppgiftsföraren ska meddela uppgiftsföraren om underentreprenören underlåter att fullgöra sina skyldigheter inom ramen för avtalet.
9.5	The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.	9.5	Uppgiftsföraren ska komma överens om en klausul om tredjepartsberättigande med underentreprenören, varigenom uppgiftsföraren – om uppgiftsföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp avtalet med underentreprenören och beordra underentreprenören att radera eller återlämna personuppgifterna.
10.	Clause 10 – Data subject rights	10.	Klausul 10 – De registrerades rättigheter
10.1	The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.	10.1	Uppgiftsföraren ska skyndsamt meddela uppgiftsföraren om varje begäran från en registrerad. Uppgiftsföraren ska inte själv besvara begäran, såvida inte han eller hon har fått tillstånd att göra detta av uppgiftsföraren.
10.2	The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.	10.2	Uppgiftsföraren ska bistå uppgiftsföraren med att fullgöra dennes skyldigheter att tillgodose de registrerades begäranden om att utöva sina rättigheter enligt förordning (EU) 2016/679. I detta avseende ska parterna fastställa lämpliga tekniska och organisatoriska åtgärder i bilaga II, med beaktande av behandlingens karaktär, genom vilka biståndet ska tillhandahållas, såväl som tillämpningsområdet för och omfattningen av det bistånd som begärs.
10.3	In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the data exporter.	10.3	När uppgiftsföraren fullgör sina skyldigheter enligt leden a och b ska han eller hon följa uppgiftsförarens instruktioner.
11.	Clause 11 – Redress	11.	Klausul 11 – Tillgång till prövning

11.1	The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.	11.1	Uppgiftsföraren ska informera de registrerade i ett öppet och lättillgängligt format, genom enskilda meddelanden eller på sin webbplats, om en kontaktpunkt som har tillstånd att hantera klagomål. Uppgiftsföraren ska skyndsamt hantera varje klagomål som tas emot från en registrerad.
11.2	In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.	11.2	Om en tvist uppstår mellan en registrerad och en av parterna när det gäller efterlevnaden av dessa klausuler ska den parten göra sitt yttersta för att lösa tvisten i godo på ett skyndsamt sätt. Parterna ska informera varandra om sådana tvister och, i tillämpliga fall, samarbeta för att lösa dem.
11.3	Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:	11.3	Om den registrerade åberopar en rättighet som berättigad tredje part enligt klausul 3 ska uppgiftsföraren godta den registrerades beslut att
11.3.1	lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;	11.3.1	inge ett klagomål till tillsynsmyndigheten i den medlemsstat där han/hon är stadigvarande bosatt eller har sin arbetsplats, eller till den behöriga tillsynsmyndigheten enligt klausul 13,
11.3.2	11.3.2. refer the dispute to the competent courts within the meaning of Clause 18.	11.3.2	hänskjuta tvisten till de behöriga domstolarna i den mening som avses i klausul 18
11.4	The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.	11.4	Parterna godtar att den registrerade får företrädas av ett organ, en organisation eller sammanslutning utan vinstsyfte enligt de villkor som fastställs i artikel 80.1 i förordning (EU) 2016/679
11.5	The data importer shall abide by a decision that is binding under the applicable EU or Member State law	11.5	Uppgiftsföraren ska följa ett beslut som är bindande enligt tillämplig lagstiftning i EU eller medlemsstaterna
11.6	The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws	11.6	Uppgiftsföraren är införstådd med att det val som gjorts av den registrerade inte kommer att påverka hans/hennes materiella och processuella rättigheter att begära prövning i enlighet med tillämplig lagstiftning.
12.	Clause 12 – Liability	12.	Klausul 12 – Ansvarsskyldighet

12.1	Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.	12.1	Varje part ska vara ansvarig inför den andra parten eller de andra parterna för eventuella skador den orsakar den andra parten eller de andra parterna genom överträdelse av dessa klausuler.
12.2	The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.	12.2	Uppgiftsinföraren ska vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsinföraren eller dess underentreprenör orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler
12.3	Notwithstanding paragraph 12.2, the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.	12.3	Utan att det påverkar led 12.2 ska uppgiftsutföraren vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsutföraren eller uppgiftsinföraren (eller dess underentreprenör) orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler. Detta påverkar inte uppgiftsutförarens ansvarsskyldighet eller, om uppgiftsutföraren är ett personuppgiftsbiträde som agerar på uppdrag av en personuppgiftsansvarig, den Personuppgiftsansvarigs ansvarsskyldighet enligt förordning (EU) 2016/679 eller förordning (EU) 2018/1725, enligt vad som är tillämpligt.
12.4	The Parties agree that if the data exporter is held liable under paragraph 12.3 for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.	12.4	Parterna är överens om att en uppgiftsutförare som enligt led c hålls ansvarig för skada som orsakats av uppgiftsinföraren (eller dess underentreprenör) ska ha rätt att återkräva den del av ersättningen från uppgiftsinföraren som motsvarar dennes ansvarsskyldighet för skadan.
12.5	Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.	12.5	Om fler än en part är ansvariga för eventuell skada som orsakats den registrerade till följd av en överträdelse av dessa klausuler ska alla ansvarsskyldiga parter vara solidariskt ansvariga, och den registrerade ska ha rätt att väcka talan i domstol mot var och en av dessa parter.

12.6	The Parties agree that if one Party is held liable under paragraph 12.5, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.	12.6	Parterna är överens om att en part som hålls ansvarig enligt led e ska ha rätt att återkräva från den andra parten eller de andra parterna den del av ersättningen som motsvarar dess/deras ansvarsskyldighet för skadan
12.7	The data importer may not invoke the conduct of a sub-processor to avoid its own liability.	12.7	Uppgiftsinföraren får inte åberopa en underentreprenörs uppförande för att undvika sitt eget ansvar
13.	Clause 13 – Supervision	13.	Klausul 13 – Tillsyn
13.1	Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose	13.1	[Om uppgiftsutföraren är etablerad i en av EU:s medlemsstater:] Den tillsynsmyndighet som har ansvar för att säkerställa uppgiftsutförarens efterlevnad av förordning (EU) 2016/679 när det gäller överföring av uppgifter, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet. [Om uppgiftsutföraren inte är etablerad i en av EU:s medlemsstater, men omfattas av det territoriella tillämpningsområdet för förordning (EU) 2016/679 i enlighet med artikel 3.2 i den förordningen, och har utsett en företrädare enligt artikel 27.1 i förordning (EU) 2016/679:] Tillsynsmyndigheten i den medlemsstat i vilken företrädaren i den mening som avses i artikel 27.1 i förordning (EU) 2016/679 är etablerad, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet. [Om uppgiftsutföraren inte är etablerad i en av EU:s medlemsstater, men omfattas av det territoriella tillämpningsområdet för förordning (EU) 2016/679 i enlighet med artikel 3.2 i den förordningen, dock utan att vara skyldig att utse en företrädare enligt artikel 27.2 i förordning (EU) 2016/679:] Tillsynsmyndigheten i en av de medlemsstater i vilken de registrerade vars personuppgifter överförs enligt dessa klausuler befinner sig i samband med utbudandet av varor eller tjänster till dem, eller i samband med att deras beteende övervakas, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet

behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

13.2 The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. Clause 14 – Local laws and practices affecting compliance with the Clauses

14.1 The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

14.2 The Parties declare that in providing the warranty in

13.2 Uppgiftsföraren samtycker till att godta den behöriga tillsynsmyndighetens behörighet och samarbeta med den i varje förfarande som syftar till att säkerställa efterlevnaden av dessa klausuler. Uppgiftsföraren samtycker i synnerhet till att svara på förfrågningar, gå med på revisioner och iaktta de åtgärder som antagits av tillsynsmyndigheten, inbegripet korrigerande och kompenserade åtgärder. Uppgiftsföraren ska ge tillsynsmyndigheten en skriftlig bekräftelse på att nödvändiga åtgärder har vidtagits.

AVSNITT III – LOKALA LAGAR OCH SKYLDIGHETER VID ÅTKOMST AV OFFENTLIGA MYNDIGHETER

14. Klausul 14 – Lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna

14.1 Parterna garanterar att de inte har någon anledning att misstänka att de lagar och förfaranden i det mottagande tredjelandet som är tillämpliga på uppgiftsförarens behandling av personuppgifter, däribland eventuella krav på att lämna ut personuppgifter eller åtgärder för att bevilja åtkomst för offentliga myndigheter, hindrar uppgiftsföraren från att fullgöra sina skyldigheter enligt dessa klausuler. Detta bygger på förutsättningen att lagar och förfaranden som är förenliga med andemeningen i de grundläggande rättigheterna och friheterna, och som inte går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda de ändamål som anges i artikel 23.1 i förordning (EU) 2016/679, inte strider mot dessa klausuler.

14.2 Genom att tillhandahålla den garanti som avses i led a intygar parterna att de

	paragraph 14.1, they have taken due account in particular of the following elements:		har tagit vederbörlig hänsyn till särskilt följande aspekter:
14.2.1	the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;	14.2.1	De särskilda omständigheterna kring överföringen, däribland behandlingskedjans längd, antalet inblandade aktörer och vilka överföringskanaler som använts; planerade vidare överföringar; typen av mottagare; ändamålet med behandlingen; de överförda personuppgifternas kategorier och format; den ekonomiska sektor inom vilken överföringen äger rum; platsen för lagring av de överförda uppgifterna.
14.2.2	the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ³ ;	14.2.2	De lagar och förfaranden i det mottagande tredjelandet – inbegripet krav på att lämna ut uppgifterna till offentliga myndigheter eller att ge sådana myndigheter åtkomst till uppgifterna – som är relevanta mot bakgrund av överföringens särskilda omständigheter samt tillämpliga begränsningar och skyddsåtgärder ³ ,
14.2.3	any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.	14.2.3	Alla relevanta avtalsenliga, tekniska eller organisatoriska skyddsåtgärder som införts för att komplettera skyddsåtgärderna enligt dessa klausuler, inbegripet åtgärder som tillämpats under överföringen och vid behandlingen av personuppgifterna i det mottagande tredjelandet.
14.3	The data importer warrants that, in carrying out the assessment under paragraph 14.2, it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.	14.3	Uppgiftsföraren garanterar att han eller hon, i samband med den bedömning som avses i led 14.2, har gjort sitt yttersta för att ge uppgiftsutföraren relevant information, och samtycker till att fortsätta att samarbeta med uppgiftsföraren för att säkerställa efterlevnaden av dessa klausuler.
14.4	The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.	14.4	Parterna är överens om att dokumentera den bedömning som avses i led 14.2 och att på begäran göra den tillgänglig för den behöriga tillsynsmyndigheten.
14.5	The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the	14.5	Uppgiftsföraren samtycker till att skyndsamt meddela uppgiftsföraren om han eller hon, efter att ha godkänt dessa klausuler och under hela avtalets

contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph 14.1, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph 14.1.

giltighetstid, har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i led 14.1, däribland efter en ändring i lagarna i tredjelandet eller en åtgärd (såsom en begäran om utlämnande av uppgifter) som antyder att en tillämpning av sådana lagar i praktiken inte stämmer överens med kraven i led 14.1.

14.6 Following a notification pursuant to paragraph 14.5, or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16.4 and 16.5 shall apply.

14.6 Efter att ha tagit emot ett meddelande i enlighet med led 14.5, eller om uppgiftsutföraren har andra anledningar att misstänka att uppgiftsinföraren inte längre kan fullgöra sina skyldigheter enligt dessa klausuler, ska uppgiftsutföraren skyndsamt fastställa lämpliga åtgärder (t.ex. tekniska eller organisatoriska åtgärder för att säkerställa säkerhet och konfidentialitet) som ska antas av uppgiftsutföraren och/eller uppgiftsinföraren för att hantera situationen. Uppgiftsutföraren ska avbryta överföringen av uppgifter om han eller hon anser att inga lämpliga skyddsåtgärder kan säkerställas för överföringen, eller efter att ha fått instruktioner från den behöriga tillsynsmyndigheten att göra det. I sådana fall ska uppgiftsutföraren ha rätt att säga upp avtalet i den mån det gäller behandling av personuppgifter enligt dessa klausuler. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat. Om avtalet sägs upp enligt denna klausul ska klausul 16.4 och 16.5 tillämpas.

15. **Clause 15 – Obligations of the data importer in case of access by public authorities**

15. **Klausul 15 – Uppgiftsinförarens skyldigheter vid åtkomst av offentliga myndigheter**

15.1 Notification

15.1 Meddelanden

15.1.1 The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

15.1.1 Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren och, om så är möjligt, den registrerade (vid behov med hjälp av uppgiftsutföraren) om han eller hon

15.1.1.1	receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or	15.1.1.1	får en rättsligt bindande begäran från en offentlig myndighet, inbegripet en rättslig myndighet, i enlighet med det mottagande landets lagstiftning om att personuppgifter som överförts enligt dessa klausuler ska lämnas ut; meddelandet ska innehålla information om de begärda personuppgifterna, den begärande myndigheten, den rättsliga grunden för begäran och det svar som lämnats, eller
15.1.1.2	becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.	15.1.1.2	får kännedom om att offentliga myndigheter har haft direkt tillgång till enligt dessa klausuler överförda personuppgifter i enlighet med det mottagande landets lagstiftning; meddelandet ska innehålla all information som uppgiftsföraren har tillgång till
15.1.2	If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.	15.1.2	Om uppgiftsföraren är förbjuden att meddela uppgiftsutföraren och/eller den registrerade enligt det mottagande landets lagstiftning samtycker uppgiftsföraren till att göra sitt yttersta för att få till stånd ett undantag från förbudet, för att kunna tillhandahålla så mycket information som möjligt inom kortast möjliga tid. Uppgiftsföraren samtycker till att dokumentera sina ansträngningar för att kunna bekräfta dem på begäran av uppgiftsutföraren.
15.1.3	Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have	15.1.3	Om det är tillåtet enligt det mottagande landets lagstiftning samtycker uppgiftsföraren till att, med jämna mellanrum under hela avtalets giltighetstid, ge uppgiftsutföraren så mycket relevant information som möjligt om de begäranden som tagits emot (i synnerhet antalet begäranden, vilken typ av uppgifter som begärts, den eller de begärande myndigheterna, om begärandena har bestridits och resultaten av bestridandena etc.).
15.1.4	The data importer agrees to preserve the information pursuant to paragraphs 15.1.1 to 15.1.3 for the duration of the contract and make it available to the	15.1.4	Uppgiftsföraren samtycker till att lagra den information som avses i leden 15.1.1–15.1.3 under hela avtalets giltighetstid och göra den tillgänglig för den behöriga tillsynsmyndigheten på begäran.

	competent supervisory authority on request.		
15.1.5	Paragraphs 15.1.1 to 15.1.3 are without prejudice to the obligation of the data importer pursuant to Clause 14.5 and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.	15.1.5	Leden 15.1.1–15.1.3 påverkar inte uppgiftsförarens skyldighet enligt klausul 14.5 och klausul 16 att skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler.
15.2	Review of legality and data minimisation	15.2	Granskning av laglighet och uppgiftsminimering
15.2.1	The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14.5.	15.2.1	Uppgiftsföraren samtycker till att granska lagligheten i begäran om utlämnande av uppgifter, särskilt om begäran omfattas av de befogenheter som har beviljats den begärande offentliga myndigheten, och att bestrida begäran om han eller hon, efter noggrann bedömning, drar slutsatsen att det finns rimliga skäl att betrakta begäran som olaglig enligt det mottagande landets lagstiftning, tillämpliga skyldigheter enligt internationell rätt och principen om internationell hövlighet. Uppgiftsföraren ska, enligt samma villkor, fullfölja möjligheterna att överklaga. Om uppgiftsföraren bestrider en begäran ska han eller hon vidta provisoriska åtgärder för att upphäva konsekvenserna av begäran tills den behöriga rättsliga myndigheten har fattat beslut i frågan. Uppgiftsföraren får inte lämna ut de begärda personuppgifterna förrän han eller hon är skyldig att göra detta enligt tillämpliga förfaranderegler. Dessa krav påverkar inte uppgiftsförarens skyldigheter enligt klausul 14.5.
15.2.2	The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.	15.2.2	Uppgiftsföraren samtycker till att dokumentera sin rättsliga bedömning och varje bestridande av begäran om utlämnande av uppgifter och, i den mån det är tillåtet enligt det mottagande landets lagstiftning, göra dokumentationen tillgänglig för uppgiftsutföraren. Uppgiftsföraren ska även göra dokumentationen tillgänglig för den behöriga tillsynsmyndigheten på begäran

15.2.3 The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

16. Clause 16 – Non-compliance with Clauses and termination

16.1 The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

16.2 In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14.6.

16.3 The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

16.3.1 the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph 16.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

16.3.2 the data importer is in substantial or persistent breach of these Clauses; or

16.3.3 the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than

15.2.3 Uppgiftsföraren samtycker till att tillhandahålla den minsta tillåtna mängden information när han eller hon besvarar en begäran om utlämnande av uppgifter, baserat på en rimlig tolkning av begäran.

AVSNITT IV - SLUTBESTÄMMELSER

16. Klausul 16 – Bristande efterlevnad av klausulerna och avtalets uppsägning

16.1 Uppgiftsföraren ska skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler, oavsett orsak.

16.2 Om uppgiftsföraren bryter mot dessa klausuler eller inte kan uppfylla kraven i dessa klausuler ska uppgiftsutföraren avbryta överföringen av personuppgifter till uppgiftsföraren tills efterlevnaden åter har säkerställts eller avtalet har sagts upp. Detta påverkar inte tillämpningen av klausul 14.6.

16.3 Uppgiftsutföraren ska ha rätt att säga upp avtalet i den mån det gäller behandlingen av personuppgifter enligt dessa klausuler om

16.3.1 uppgiftsutföraren har avbrutit överföringen av personuppgifter till uppgiftsföraren enligt led 16.2 och om efterlevnaden av dessa klausuler inte har återupprättats inom en rimlig tidsperiod, under alla omständigheter inom en månad efter avbrytandet,

16.3.2 uppgiftsföraren gör sig skyldig till allvarliga eller upprepade överträdelser av dessa klausuler, eller

16.3.3 uppgiftsföraren inte följer ett bindande beslut av en behörig domstol eller tillsynsmyndighet angående hans eller hennes skyldigheter enligt dessa klausuler.

I sådana fall ska uppgiftsutföraren informera den behöriga tillsynsmyndigheten [för modul tre: och den Personuppgiftsansvarig] om denna

two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

bristande efterlevnad. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat.

16.4 Personal data that has been transferred prior to the termination of the contract pursuant to 16.3 shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

16.4 Personuppgifter som överförts före uppsägningen av avtalet i enlighet med led 16.3 ska efter uppgiftsutförarens eget val omedelbart återlämnas till uppgiftsutföraren eller raderas i sin helhet. Detsamma ska gälla för eventuella kopior av uppgifterna. Uppgiftsinföraren ska intyga för uppgiftsutföraren att uppgifterna har raderats. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av de överförda personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen.

16.5 Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

16.5 Endera parten får återkalla sin överenskommelse om att vara bunden av dessa klausuler om i) Europeiska kommissionen antar ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679 som omfattar den överföring av personuppgifter som dessa klausuler gäller för, eller ii) förordning (EU) 2016/679 blir en del av den rättsliga ramen i det land till vilket personuppgifterna överförs. Detta påverkar inte övriga skyldigheter som är tillämpliga på behandlingen i fråga enligt förordning (EU) 2016/679.

17. Clause 17 – Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be

17. Klausul 17 – Tillämplig lag

Dessa klausuler ska regleras genom lagstiftningen i den medlemsstat i EU i vilken uppgiftsutföraren är etablerad. Om lagstiftningen inte omfattar rättigheter för berättigade tredje parter ska klausulerna regleras genom

governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of [REDACTED].

lagstiftningen i en annan medlemsstat i EU som omfattar rättigheter för berättigade tredje parter. Parterna är överens om att detta ska vara lagstiftningen i [REDACTED].

18. Clause 18 – Choice of forum and jurisdiction

18. Klausul 18 – Val av forum och jurisdiktion

18.1 Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

18.1 Varje tvist som uppstår på grund av dessa klausuler ska lösas av domstolarna i en medlemsstat i EU.

18.2 The Parties agree that those shall be the courts of [REDACTED].

18.2 Parterna är överens om att dessa ska vara domstolarna i [REDACTED].

18.3 A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

18.3 En registrerad får även inleda rättsliga förfaranden mot uppgiftsutföraren och/eller uppgiftsinföraren vid domstolarna i den medlemsstat där han/hon har sin stadigvarande vistelseort.

18.4 The Parties agree to submit themselves to the jurisdiction of such courts.

18.4 Parterna är överens om att underkasta sig sådana domstolars jurisdiktion.

APPENDIX to the Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Identity and contact details of the Controller and, where applicable, of its/their data protection officer and/or representative in the European Union

- (i) Name
- (ii) Address
- (iii) Contact person's name, position and contact details
- (iv) Activities relevant to the data transferred under these Clauses
- (v) Signature and date
- (vi) Role (controller/processor)

Data importer(s): Identity and contact details of the Processor, including any contact person with responsibility for data protection

- (i) Name: SMART Technologies ULC
- (ii) Address: 3636 Research Road NW, Calgary B, T2L 1Y1
- (iii) Contact person's name, position, and contact details: Glenn Carbol, Data Protection Officer
- (iv) Activities relevant to the data transferred under these Clauses: Processing of data for SMART Learning Suite
- (v) Signatures and date: [REDACTED]
- (vi) Role (controller/processor): Processor

TILLÄGG

BILAGA I

A. FÖRTECKNING ÖVER PARTER

Uppgiftsutförare:
Uppgiftsutförarens/uppgiftsutförarnas identitet och kontaktuppgifter och, i tillämpliga fall, uppgifter om hans/hennes eller deras dataskyddsombud och/eller företrädare i Europeiska unionen

- (i) Namn
- (ii) Adress
- (iii) Kontaktpersonens namn, befattning och kontaktuppgifter
- (iv) Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler
- (v) Underskrift och datum
- (vi) Roll
(personuppgiftsansvarig/personuppgiftsbiträde)

Uppgiftsinförare:
Uppgiftsinförarens/uppgiftsinförarnas identitet och kontaktuppgifter, inklusive eventuella kontaktpersoner med ansvar för dataskydd

- (i) Namn: SMART Technologies ULC
- (ii) Adress: 3636 Research Road NW, Calgary B, T2L 1Y1
- (iii) Kontaktpersonens namn, befattning och kontaktuppgifter: Glenn Carbol, Data Protection Officer
- (iv) Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler Processing of data for SMART Learning Suite
- (v) Underskrift och datum: [REDACTED]
- (vi) Roll
(personuppgiftsansvarig/personuppgiftsbiträde): personuppgiftsbiträde

B. DESCRIPTION OF TRANSFER**Categories of data subjects whose personal data are transferred**

- (i) User
- (ii) Customer

Categories of personal data transferred**User**

- (i) Direct identifying information (e.g. name, email address)
- (ii) Any personal data supplied by end users of the Service
- (iii) Application Technology Meta Data
 - a. IP addresses, use of cookies, etc.
- (iv) Application Use Statistics
 - a. Meta data on user interaction with application
 - b. Other assessment data – determined by teacher running the class
- (v) Online communications captured (emails, blog entries)
- (vi) Provder/App assigned student ID number
- (vii) Student app username
- (viii) Student responses to surveys or questionnaires
- (ix) Student generated content; writing, pictures, etc. – anything stored in teacher's lesson file
- (x) Microsoft Single Sign-On
- (xi) Google Single Sign-On
- (xii) Region for data storage (USA or EU)
- (xiii) Google Analytics (anonymous)
- (xiv) MixPanel Analytics (anonymous)

Categories of Data Subjects for Customers

- (i) Organization name

B. BESKRIVNING ÖVERFÖRINGEN**AV****Kategorier av registrerade vars personuppgifter överförs**

- (i) Användare
- (ii) Kunder

Kategorier av personuppgifter som överförs**Användare**

- (i) Direkt identifierande information (namn, e-postadress)
- (ii) Personuppgifter från slutanvändare av Tjänsten
- (iii) Applikationsteknisk metadata
 - a. IP-adresser, användning av kakor etc.
- (iv) Appanvändningsstatistik
 - a. Metadata över användarinteraktion med applikationen
 - b. Annan bedömningsdata som bestämts av kursansvarige
- (v) Upptagen onlinekommunikation (epost, blogginlägg)
- (vi) Student-ID kopplad till Provder/applikation
- (vii) Studentanvändarnamn på applikation
- (viii) Studenters svar på undersökningar eller frågeformulär
- (ix) Studentgenererat innehåll såsom skrift, bilder, etc. – allt som finns lagrat på kursansvariges klassmapp.
- (x) Microsoft Single Sign-On
- (xi) Google Single Sign-On
- (xii) Region för datainsamling (EU eller USA)
- (xiii) Google Analytics (anonymiserad)
- (xiv) MixPanel Analytics (anonymiserad)

Kategorier av datasubjekt för kunder

- (i) Organisationens namn

- (ii) E-mail
- (iii) Phone
- (iv) Address
- (v) Required order information: product, quantity, price and tax, delivery

Sensitive Data

The Processor hereby expressly prohibits the Controller from transferring any special categories of personal data to it.

Frequency of the Transfer

Continuous during the Service.

Nature of the Processing

Processor will perform the following basic processing activities:

- (i) processing to provide the Service in accordance with the TOSP;
- (ii) processing to perform any steps necessary for the performance of the Service; and
- (iii) processing to comply with other reasonable instructions provided by Controller (e.g. via email) that are consistent with the terms of the TOSP.

Period for which the personal data will be retained

Throughout the Term of the TOSP plus the period from expiry of the Term until deletion of Personal Data by the Processor in accordance with applicable law or as requested by Controller (Data Erasure Request).

**C. COMPETENT
AUTHORITY**

SUPERVISORY

- (ii) E-post
- (iii) Telefonnummer
- (iv) Adress
- (v) Nödvändig orderinformation: produkt, antal, pris och skatt, leverans

Känsliga uppgifter

Personuppgiftsbiträdet förbjuder uttryckligen Personuppgiftsansvarig från att överföra särskilda kategorier av personuppgifter till personuppgiftsbiträdet.

Frekvens för överföringen

Kontinuerligt under Tjänstens tillhandahållande.

Behandlingens karaktär

Personuppgiftsansvarige kommer utföra de följande grundläggande behandlingarna:

- (i) behandling för att erbjuda Tjänsten i enlighet med Huvudavtalet,
- (ii) behandling för att genomföra steg nödvändiga för att erbjuda Tjänsten, och
- (iii) behandling för att säkra efterlevnad med Personuppgiftsansvarigs andra rimliga instruktioner (exempelvis via e-post) som överensstämmer med föreskrifterna i Huvudavtalet.

Den period under vilken personuppgifterna kommer att lagras

Under Huvudavtalets löptid samt under den period form löptidens upphörande fram till dess att personuppgifterna raderas av personuppgiftsbiträdet i enlighet med tillämplig lag eller på Personuppgiftsansvarigs begäran (gallringsbegäran).

C.

BEHÖRIG TILLSYNSMYNDIGHET

Identify the competent supervisory authority/ies in accordance with Clause 13:

Controller please enter your country's supervisory authority here:

**Note - where the Controller acts as the data exporter and is established in an EU Member State the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated here, shall act as competent supervisory authority.*

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Parties shall agree the following categories of measures will be implemented. The details of each measure is available upon request.

- 1 The Processor should have a structured organisation where different employees have roles and responsibilities regarding security information that are clearly defined.
- 2 The Processor shall on a regular basis provide courses to increase awareness regarding information systems built to resist.
- 3 The Processor should have routines and functions in order to permanently delete and erase information that is related to the delivery.
- 4 The Processor has performed a risk evaluation of the system and performed measurements to identify any faults in such system
- 5 The Controller's requirements regarding processing of information shall be adopted. In case such requirements are

Ange den eller de behöriga tillsynsmyndigheterna i enlighet med klausul 13.

Personuppgiftsansvarig, vänligen
uppgift ert lands
dataskyddsmyndighet: [REDACTED].

*Notera – då Personuppgiftsansvarig agerar som uppgiftsutförare och är etablerad i ett medlemslands skall tillsynsmyndigheten med ansvar för efterlevnad för uppgiftsutföraren under Europaparlamentets och rådets förordning (EU) 2016/670, som indikerat, agera som tillsynsmyndighet.

BILAGA II – TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INKLUSIVE TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA UPPGIFTERNAS SÄKERHET

Parterna skall vara överens om att följande åtgärds-kategorier skall implementeras. Detaljer kring varje åtgärds-kategori finns tillgänglig på begäran.

- 1 Personuppgiftsbiträdet borde ha en strukturerad organisation där olika anställda har roller och ansvarsområden avseende säkerhetsinformation som är klart definierade.
- 2 Personuppgiftsbiträdet skall med regelbundenhet erbjuda kurser för att öka medvetenheten kring motståndskraftiga informationssystem.
- 3 Personuppgiftsbiträdet borde ha rutiner och funktioner för att permanent kunna radera permanent uppgifter som är relaterade till leveransen.
- 4 Personuppgiftsbiträdet has utfört en riskutvärdering av systemet och vidtagit åtgärder för att identifiera brister i systemet
- 5 Personuppgiftsansvarigs krav för behandling av uppgifter skall adopteras. In det fall sådana krav inte

	not expressed, the Processor shall be able to present the routines that apply to the Processor.		framställs ska Personuppgiftsbiträdet på egen hand ta fram de nödvändiga rutinerna för Personuppgiftsbiträdet.
6	The users are to be provided personal and unique user identities to the extent that anonymous guest accounts are to not used. For more information, see Guidance for trust level 1 (LoA1).	6	Användarna skall ges personliga och unika användaridentiteter i de fall där anonyma gästkonton inte används. För mer information, se Riktlinjer för förtroendenivå 1 (LoA1)
7	The Processor shall follow an agreed upon routine that enables the Controller to approve certain selected authorities.	7	Personuppgiftsbiträdet skall följa en förutbestämd rutin som möjliggör för Personuppgiftsansvarig att godkänna vissa utvalda auktoriteter.
8	The Processor shall use personal and traceable user identities for high level authorities that are used to administrate the system.	8	Personuppgiftsbiträdet skall använda personliga och spårbara användaridentiteter för höghöjdsauktoriteter som används för att administrera systemet.
9	The Processor shall have a system that distributes and resets passwords without disclosing the password to unauthorised persons. For more information, see Guidance for trust level 1 (LoA1).	9	Personuppgiftsbiträdet skall ha ett system som fördelar och återställer lösenord utan att uppge lösenordet för obehöriga individet. För mer information se Riktlinjer för förtroende nivå 1 (LoA1)
10	The authorisation system shall log information of when a user is created or removed.	10	Auktoriseringssystemet skall logga information kring när en användare skapas och när en användare tas bort.
11	The Processor shall have a routine for removing user identities from the system.	11	Personuppgiftsbiträdet skall ha en rutin för att ta bort användaridentiteter från systemet.
12	The Processor shall have established rules regarding the person responsible for handling authentication information.	12	Personuppgiftsbiträdet skall ha etablerat regler kring den individ som är ansvarig för hanterandet av auktoriseringsinformation.
13	Only information or services that are public shall be available in the system and any other related infrastructure that has not been subject to authentication.	13	Bara information eller tjänster som är offentliga skall vara tillgängliga i systemet och all annan därtill relaterad infrastruktur som inte har utsatts för auktorisering.
14	The system shall use passwords or anything that holds a better security level for authentication. There should be provided rules for how a password is allowed to be handled in the system and by a user. For more information, see Guidance for trust level 1 (LoA1).	14	Systemet skall använda sig av lösenord eller något annat som håller en högre säkerhetsnivå för auktorisering. Regler borde föras för hur ett lösenord ska behandlas i systemet och av en användare. För mer information se Riktlinjer för förtroendenivå 1 (LoA1)

15	The so called data hall shall fulfil at least protection level 2 (according to "data room", stated in the Swedish Civil Contingencies Agencies "Guidance for physical security information in the it-room").	15	Den s.k. datorhallen skall uppnå som lägst skyddsnivå 2 (i enlighet med "data room", uttalat i Myndigheten för samhällsskydd och beredskaps "Vägledning för fysisk informationssäkerhet i IT-utrymmen")
16	The Processor shall have routines in which secure that only authorised personal have physical access to the so called data hall.	16	Personuppgiftsbiträdet skall ha rutiner som försäkrar att bara auktoriserad personal har fysisk tillgång till den s.k. datorhallen.
17	The Processor should have different functions, processes and routines to monitor and create prognoses regarding performance.	17	Personuppgiftsbiträdet skall ha olika funktioner, processer och rutiner för övervakning och för att skapa prognoser för prestation.
18	The Processor should provide protection against damaging code for the parts that are included in the delivery.	18	Personuppgiftsbiträdet skall tillhandahålla skydd mot skadlig kod för de parter som är inkluderade i leveransen.
19	The Processor should have routines and functions for backups and restoration of information according to the agreed upon accessibility requirements with the Controller. Backups should be protected in the same way as the original information and stored separately.	19	Personuppgiftsbiträdet skall ha rutiner och funktioner för säkerhetskopiering och restorering av uppgifter i enlighet med de tillgänglighetskrav man kommit överens om tillsammans med Personuppgiftsansvarig. Säkerhetskopiorna skall skyddas på samma sätt som originalen och bör förvaras separat från originalen.
20	Log-in functions should be available for security related events, especially regarding incorrect log-ins, any change to an authorisation, unauthorised connections and infringements of authorisations.	20	Inloggningsfunktioner skall vara tillgängliga för säkerhetsrelaterade händelser, särskild sådana som rör felaktiga inloggningar, förändrade auktoriseringar, obehöriga uppkopplingar och överträdelser av behörigheter.
21	The Processor shall protect log-in functions and log tools against manipulation and unauthorised access, which also includes the Processor's employees.	21	Personuppgiftsbiträdet skall skydda inloggningsfunktioner och loggningsverktyg mot manipulation och obehörig tillgång. Detta inbegriper även Personuppgiftsbitrådets anställda.
22	The system and related infrastructure should use the same time synchronisation as the time source, which is UTC+0.	22	Systemet och därtill hörande infrastruktur skall använda samma tidssynkronisering som tidskällan, vilket är UTC+0,
23	The Processor shall without delay inform the Controller about technical vulnerabilities in the delivered components. Found vulnerabilities should be amended immediately.	23	Personuppgiftsbiträdet skall utan dröjsmål informera Personuppgiftsansvarig om tekniska svagheter i levererade delar. Upptäckta svagheter skall åtgärdas omedelbart.

- 24 The Controller shall upon request be informed about every exchange of information that occurs with other systems outside the Controller's environment.
- 25 The Processor has established and documented principles and methods for the development of secure systems and present these to the Controller.
- 26 The Processor has guidelines for an information system to resist within their development processes.
- 27 The Processor's responsibilities as stated herein will apply to any sub-processors. The Controller shall upon request be informed of which sub-processor is used.

ANNEX III – SUB-PROCESSORS

The Controller has authorised the use of the following sub-processors.

LIST OF SUB-PROCESSORS:
<https://www.smarttech.com/legal/lumio-privacy>

GUESTS

Self-Chosen Display Name for Guests

Type	Anonymous
Where	Who

Canada	SMART Technologies ULC
--------	------------------------

Data/Purpose: Required for basic functionality. Display name is recorded inside of a teacher's lesson or activity when the user participates.
 SLS Terms
 GDPR - EC Adequacy Decision

USA/Germany	Amazon Web Services, Inc
-------------	--------------------------

- 24 Personuppgiftsansvarig skall på begäran informeras om varje informationsutbyte som sker med andra system utanför Personuppgiftsbitrådets miljö.
- 25 Personuppgiftsbitrådet har etablerat och dokumenterat principer och metoder för utvecklingen av säkra system och presenterat dessa för Personuppgiftsansvarig.
- 26 Personuppgiftsbitrådet har riktlinjer för ett informationssystem motståndskraft inom ramen för deras utvecklingsprocess.
- 27 Personuppgiftsbitrådets ansvar enligt vad som framgår här skall även gälla för eventuella underbiträden. Personuppgiftsansvarig skall på begäran bli informerad om vilka underbiträden som engagerats.

BILAGA III – FÖRTECKNING ÖVER UNDERENTREPRENÖRER

Den personuppgiftsansvarige har gett tillstånd att använda följande underentreprenörer:

LISTA ÖVER UNDERENTREPRENÖRER:
<https://www.smarttech.com/legal/lumio-privacy>

GÄSTER

Egenvalt visningsnamn för gäster

Typ	Anonym
Var	Vem

Kanada	Smart Technologies ULC
--------	------------------------

Information/syfte: Nödvändig för grundfunktionalitet. Visningsnamn spelas in under lärarledd lektion eller aktivitet då användaren deltar.
 SLS-villkor
 GDPR – EC Adequacy Decision

USA/Germany	Amazon Web Services, Inc
-------------	--------------------------

Data/Purpose: Required for storage. We offer both an American and European data storage option.
AWS Privacy
AWS GDPR

USA/Belgium Firebase (Google LLC)

Data/Purpose: Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing).
Firebase Privacy
Firebase GDPR

Guest Created Content

Type *Anonymous*
Where *Who*

Canada SMART
Technologies ULC

Data/Purpose: Required for basic functionality. Display name is recorded inside of a teacher's lesson or activity when the user participates.
SLS Terms
GDPR - EC Adequacy Decision

USA/Germany Amazon Web Services, Inc

Data/Purpose: Required for storage. We offer both an American and European data storage option.
AWS Privacy
AWS GDPR

USA/Belgium Firebase (Google LLC)

Data/Purpose: Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing).
Firebase Privacy
Firebase GDPR

Guest Analytics

Information/syfte: Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska dalalagringsalternativ.
AWS sekretess
AWS GDPR

USA/Belgien Firebase(Google LLC)

Information/syfte: Nödvändig för grundfunktionalitet (Firebase är Backend-as-a-service (BaaS) cloud-computing-lösning som vi använder för automatiserade datorprocesser i realtid (tillfälligt)
Firebase sekretess
Firebase GDPR

Gästskapat innehåll

Typ *Anonym*
Var *Vem*

Kanada Smart Technologies
ULC

Information/syfte: Nödvändig för grundfunktionalitet. Visningsnamn spelas in under lärarledd lektion eller aktivitet då användaren deltar.
SLS-villkor
GDPR – EC Adequacy Decision

USA/Germany Amazon Web Services, Inc

Information/syfte: Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska dalalagringsalternativ.
AWS sekretess
AWS GDPR

USA/Belgien Firebase(Google LLC)

Data/syfte: Nödvändig för grundfunktionalitet (Firebase är Backend-as-a-service (BaaS) cloud-computing-lösning som vi använder för automatiserade datorprocesser i realtid (tillfälligt)
Firebase sekretess
Firebase GDPR

Användaranalys

Type Anonymous
Where Who

Canada SMART
Technologies ULC

Data/Purpose: Required for basic functionality. Display name is recorded inside of a teacher's lesson or activity when the user participates.
SLS Terms
GDPR - EC Adequacy Decision

USA Mixpanel, Inc.

Data/Purpose: Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime.
Mixpanel Privacy
Mixpanel GDPR

N/A Third part content providers

Data/purpose: Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.

USA Sentry.io

Data/Purpose:

Typ Anonym
Var Vem

Kanada Smart Technologies
ULC

Information/syfte: Nödvändig för grundfunktionalitet. Visningsnamn spelas in under lärarledd lektion eller aktivitet då användaren deltar.
SLS-villkor
GDPR – EC Adequacy Decision

USA Mixpanel, Inc.

Information/syfte: Information/syfte: Nödvändig för produktutveckling och övervakning av tjänst. Mixpanel tillåter oss att analysera hur våra oidentifierade användare interagerar med Lumio. Det är designat för att identifiera trender, förstå sammanslagna aggregerade användarbeteenden och hjälper oss att ta bättre beslut kring hur användarvänligheten och funktioner i vår produkt kan förbättras. Denna information används även för att mäta hur lång tid det tar för våra servrar att slutföra handlingar som att öppna filer, vilket hjälper oss mäta tjänstens status och up/downtime.
Mixpanel sekretess
Mixpanel GDPR

N/A tredje part som skapar innehåll

Information/syfte: Valbart innehåll eller aktivitet som en lärare kan lägga till en lektion, såsom en YouTube-video eller annat inbäddat innehåll en användare frivilligt lägger till. Vi kan ej kontrollera vad för slags information tredje part direkt samlar in när en lärare eller student väljer att inkludera den typen av innehåll i en lektion. SMART utfäster, dock, att vi bara rapporterar anonymt användande till tredje part.

USA Sentry.io

Information/syfte:

- (i) Lesson ID (no PII)
- (ii) User ID and Session IDs (hashed and salted to maintain anonymity)
- (iii) request header (application and version, platform, operating system, browser, language, date and time)
- (iv) bread crumbs (last pages visited and links clicked)

Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

STUDENTS/MINOTS, SIGNED IN

Student account

Type *Anonymous*
Where *Who*

Canada SMART
Technologies ULC

Data/Purpose: Required account details for product functionality: display name, full name, email, public profile picture. language preference.

SLS Terms

GDPR - EC Adequacy Decision

Global Microsoft, Inc.

Data/Purpose: Required if you use Microsoft as your single-sign-on (SSO) provider to access Lumio. Microsoft provides SMART with required account details.

Microsoft SSO

Microsoft Privacy

Microsoft GDPR

Global Google LLC

- (i) Lektions-ID (inget PII)
- (ii) Användar-ID och sessions-ID (hashed samt salted i syfte att upprätthålla anonymitet)
- (iii) Request header (applikation och version, plattform, operativsystem, webbläsare, språk, datum och tid)
- (iv) Bread crumbs (senaste besökta sidor och klickade länkar)

Valfri rapportering av användarfel: Efter att en automatiserat felrapport är sammanställd så ges användare möjligheten att bidra med sina namn, e-post adresser samt annan tilläggsinformation kring felet. Användare ombeds även svara på om de vill att SMART gör en uppföljning med dem. Dessa valfria personuppgifter lagras i Salesforce (lokaliserat i USA) och delas med vårt kundtjänst-team.

STUDENTER/MINDERÅRIGA, INLOGGADE

Studentkonto

Typ *Anonym*
Var *Vem*

Kanada Smart Technologies
ULC

Information/syfte: Nödvändiga kontodetaljer för produktfunktionalitet: visningsnamn, för- och efternamn, e-post adress, public profilbild, språkpreferenser.

SLS-villkor

GDPR – EC Adequacy Decision

Globalt Microsoft, Inc.

Information/syfte: Nödvändig om du använder Microsoft som din tillhandahållare för single-sign-on (SSO) för åtkomst till Lumio. Microsoft tillhandahåller SMART med nödvändiga kontodetaljer.

Microsoft SSO

Microsoft sekretess

Microsoft GDPR

Global Google LLC

Data/Purpose: Required if you use Google as your single-sign-on (SSO) provider to access Lumio. Google provides SMART with required account details.

Google SSO
Google Privacy
Google GDPR

USA/Germany Amazon Web Services, Inc.

Required for storage. We offer both an American and European data storage option.

AWS Privacy
AWS GDPR

Using Lumio as a Signed-In Student (student created content)

Type *Anonymous*
Where *Who*

Canada SMART Technologies ULC

Data/Purpose: Optional. If students participate in live activities where they provide responses or they upload content they created, it will be attributed to their account.

SLS Terms
GDPR - EC Adequacy Decision

USA/Germany Amazon Web Services, Inc

Data/Purpose: Required for storage. We offer both an American and European data storage option.

AWS Privacy
AWS GDPR

USA/Belgium Firebase (Google LLC)

Data/Purpose: Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing).

Information/syfte: Nödvändig om du använder Google som din tillhandahållare för single-sign-on (SSO) för åtkomst till Lumio. Google tillhandahåller SMART med nödvändiga kontodetaljer.

Google SSO
Google sekretess
Google GDPR

USA/Germany Amazon Web Services, Inc.

Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska datalagringsalternativ.

AWS Privacy
AWS GDPR

Att använda Lumio som inloggad student (innehåll skapat av studenten)

Typ *Anonym*
Var *Vem*

Kanada Smart Technologies ULC

Information/syfte: Valfri. Om studenter deltar i aktiviteter i realtid där de utger svar eller laddar upp innehåll de själva skapat så kommer det hänföras till deras konto.

SLS-villkor
GDPR – EC Adequacy Decision

USA/Germany Amazon Web Services, Inc

Information/syfte: Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska datalagringsalternativ.

AWS sekretess
AWS GDPR

USA/Belgium Firebase(Google LLC)

Data/syfte: Nödvändig för grundfunktionalitet (Firebase är Backend-as-a-service (BaaS) cloud-computing-lösning som vi använder

Firebase Privacy
Firebase GDPR

för automatiserade datorprocesser i
realtid (tillfälligt)
Firebase sekretess
Firebase GDPR

Signed-In Student Analytics

Type *Anonymous*
Where *Who*

Canada SMART
Technologies ULC

Data/Purpose: Required for product improvement and service monitoring. We use Mixpanel as our processor for this.
SLS Terms
GDPR - EC Adequacy Decision

USA Mixpanel, Inc.

Data/Purpose: Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime.
Mixpanel Privacy
Mixpanel GDPR

N/A Third party content providers

Data/Purpose: Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects via the content when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.

Analys av inloggade studenter

Typ *Anonym*
Var *Vem*

Kanada Smart Technologies
ULC

Information/syfte: Nödvändig för produktförbättring och övervakning av tjänst. Vi använder Mixpanel som vårt personuppgiftsbiträde för detta.
SLS-villkor
GDPR – EC Adequacy Decision

USA Mixpanel, Inc.

Information/syfte: Nödvändig för produktförbättring och övervakning av tjänst. Mixpanel tillåter oss att analysera hur våra oidentifierade användare interagerar med Lumio. Det är designat för att identifiera trender, förstå sammanslagna aggregerade användarbeteenden och hjälper oss att ta bättre beslut kring hur användarvänligheten och funktioner i vår produkt kan förbättras. Denna information används även för att mäta hur lång tid det tar för våra servrar att slutföra handlingar som att öppna filer, vilket hjälper oss mäta tjänstens status och up/downtime.
Mixpanel sekretess
Mixpanel GDPR

N/A tredje part som
tillhandahåller innehåll

Information/syfte: Valfritt innehåll eller valfri aktivitet som en lärare lägger till en lektion, såsom en YouTube-video eller annat inbäddat innehåll en användare frivilligt lägger till. Vi kan ej kontrollera vilken information tredje part samlar in direkt via den innehållet när en lärare eller student beslutar att inkludera innehållet i en lektion. För premiuminnehåll SMART tillhandahåller gäller dock att vi bara rapporterar anonymt användande till tredje part.

USA Sentry.io

Data/Purpose:

- (i) Lesson ID (no PII)
- (ii) User ID and Session IDs (hashed and salted to maintain anonymity)
- (iii) request header (application and version, platform, operating system, browser, language, date and time)
- (iv) bread crumbs (last pages visited and links clicked)

Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

TEACHER/ADULT, SIGNED IN

Teacher Account

Type Anonym
Where Who

Canada SMART
Technologies ULC

Data/purpose: Required account details: display name, name, email, public profile picture. language preference. Required account profile settings: opt-ins, user type, location.
SLS Terms
GDPR - EC Adequacy Decision

Global Microsoft, Inc.

Data/Purpose: Required if you use Microsoft as your single-sign-on (SSO) provider to access Lumio. Microsoft provides SMART with required account details.
Microsoft SSO

USA Sentry.io

Information/syfte:

- (i) Lektions-ID (ingen PII)
- (ii) Användar-ID och sessions-ID (hashed och salted i syfte att bibehålla anonymitet)
- (iii) Request header (application och version, plattform, operativsystem, webbläsare, spark, datum och tid)
- (iv) Bread crumbs (senast besökta sidorna och klickade länkar)

Valfri rapportering av användarfel: Efter att en automatiserat felrapport är sammanställd så ges användare möjligheten att bidra med sina namn, e-post adresser samt annan tilläggsinformation kring felet. Användare ombeds även svara på om de vill att SMART gör en uppföljning med dem. Dessa valfria personuppgifter lagras i Salesforce (lokaliserat i USA) och delas med vårt kundtjänst-team.

LÄRARE/MYNDIG, INLOGGAD

Lärarkonto

Typ Anonym
Var Vem

Kanada Smart Technologies
ULC

Information/syfte: Nödvändiga kontodetaljer: visningsnamn, namn, e-post adress, public profilbild, språkpreferenser. Nödvändiga kontoinställningar, opt-ins, användartyp, plats.
SLS-villkor
GDPR -EC Adequacy Decision

Globalt Microsoft, Inc.

Information/syfte: Nödvändig om du använder Microsoft som din tillhandahållare för single-sign-on (SSO) för åtkomst till Lumio. Microsoft tillhandahåller SMART med nödvändiga kontodetaljer.

Microsoft Privacy
Microsoft GDPR

Global Google LLC

Data/Purpose: Required if you use Google as your single-sign-on (SSO) provider to access Lumio. Google provides SMART with required account details.

Google SSO
Google Privacy
Google GDPR

USA/Germany Amazon Web
Services, Inc.

Data/Purpose: Required for storage. We offer both an American and European data storage option.

AWS Privacy
AWS GDPR

Using Lumio as a Signed-In Teacher (Teacher created content)

Type *Anonymous*
Where *Who*

Canada SMART
Technologies ULC

Data/Purpose: Generated Content (lessons and activities created by a teacher). Self-chosen class names.

SLS Terms
GDPR - EC Adequacy Decision

USA/Germany Amazon Web Services,
Inc

Data/Purpose: Required for storage. We offer both an American and European data storage option.

AWS Privacy
AWS GDPR

USA/Belgium Firebase (Google LLC)

Data/Purpose: Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing

Microsoft SSO
Microsoft Privacy
Microsoft GDPR

Global Google LLC

Information/syfte: Nödvändig om du använder Google som din tillhandahållare för single-sign-on (SSO) för åtkomst till Lumio. Google tillhandahåller SMART med nödvändiga kontodetaljer.

Google SSO
Google Privacy
Google GDPR

USA/Germany Amazon Web
Services, Inc.

Innehåll/syfte: Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska dalalagringsalternativ.

AWS sekretess
AWS GDPR

Att använda Lumio som inloggad lärare (innehåll skapat av läraren)

Typ *Anonym*
Var *Vem*

Canada SMART
Technologies ULC

Innehåll/syfte: Genererat innehåll (lektioner och aktiviteter skapade av en lärare). Självvalda klassnamn.

SLS-villkor
GDPR- EC Adequacy Decision

USA/Germany Amazon Web
Services, Inc

Information/syfte: Nödvändig för lagring. Vi erbjuder både amerikanska och europeiska dalalagringsalternativ.

AWS sekretess
AWS GDPR

USA/Belgium Firebase (Google
LLC)

Information/syfte: Nödvändig för grundfunktionalitet (Firebase är Backend-as-a-service (BaaS) cloud-computing-lösning som vi använder

solution we use for real time (temporary) automated computer processing).
Firebase Privacy
Firebase GDPR

Signed-In Teacher Analytics

Type Pseudonymized
Where Who

Canada SMART
Technologies ULC

Data/Purpose: Required for product improvement and service monitoring. We use Mixpanel as our processor for this.
SLS Terms
GDPR - EC Adequacy Decision

USA Mixpanel, Inc.

Data/Purpose: Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime.
Mixpanel Privacy
Mixpanel GDPR

N/A Third party content providers

Data/Purpose: Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects via the content when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.

USA Sentry.io

för automatiserade datorprocesser i realtid (tillfälligt)
Firebase sekretess
Firebase GDPR

Analys av inloggade lärare

Typ Pseudomiserad
Var Vem

Kanada Smart Technologies
ULC

Information/syfte: Nödvändig för produktförbättring och övervakning av tjänst. Vi använder Mixpanel som vårt Personuppgiftsbiträde för detta.
SLS-villkor
GDPR – EC Adequacy Decision

USA Mixpanel, Inc.

Information/syfte: Nödvändig för produktförbättring och övervakning av tjänst. Mixpanel tillåter oss att analysera hur våra oidentifierade användare interagerar med Lumio. Det är designat för att identifiera trender, förstå sammanslagna aggregerade användarbeteenden och hjälper oss att ta bättre beslut kring hur användarvänligheten och funktioner i vår produkt kan förbättras. Denna information används även för att mäta hur lång tid det tar för våra servrar att slutföra handlingar som att öppna filer, vilket hjälper oss mäta tjänstens status och up/downtime.

N/A tredje part som
tillhandahåller innehåll

Information/syfte: Valbart innehåll eller aktivitet som en lärare kan lägga till en lektion, såsom en YouTube-video eller annat inbäddat innehåll en användare frivilligt lägger till. Vi kan ej kontrollera vad för slags information tredje part direkt samlar in när en lärare eller student väljer att inkludera den typen av innehåll i en lektion. För premiuminnehåll som SMART tillhandahåller rapporterar vi dock bara anonymiserat användande till tredje part.

USA Sentry.io

Data/Purpose:

- (i) Lesson ID (no PII)
- (ii) User ID and Session IDs (hashed and salted to maintain anonymity)
- (iii) request header (application and version, platform, operating system, browser, language, date and time)
- (iv) bread crumbs (last pages visited and links clicked)

Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

CUSTOMER DATA COLLECTED AND PROCESSED

Where: N/A

Who: Reseller & SMART's Regional Office

Role: Seller

Data/Purpose: Required contact information: organization name, e-mail, title, phone, address. Required order information: product, quantity, price and tax, delivery. Ask your local regional reseller about their privacy policies.

Typ: Identifiable

Where: Canada

Who: SMART Technologies ULC

Role: Manufacturer

Data/Purpose: Required account information: organization name, e-mail, title, phone, address, reseller, current

Information/syfte:

- (i) Lektions-ID (ingen PII)
- (ii) Användar-ID och sessions-ID (hashed och salted I syfte att bibehålla anonymitet)
- (iii) Request header (application och version, plattform, operativsystem, webbläsare, spark, datum och tid)
- (iv) Bread crumbs (senast besökta sidorna och klickade länkar)

Valfri rapportering av användarfel: Efter att en automatiserat felrapport är sammanställd så ges användare möjligheten att bidra med sina namn, e-post adresser samt annan tilläggsinformation kring felet. Användare ombeds även svara på om de vill att SMART gör en uppföljning med dem. Dessa valfria personuppgifter lagras i Salesforce (lokaliserat i USA) och delas med vårt kundtjänst-team.

KUNDDATA SO SAMLAS IN OCH BEHANDLAS

Var: N/A

Vem: Återförsäljare och SMART:s regionkontor

Roll: Säljare

Information/Syfte: Nödvändig kontaktinformation: organisationsnamn, e-post-adress, befattning, telefonnummer, adress. Nödvändig orderinformation: produkt, antal, pris och skatt, leverans. Fråga din regionala återförsäljare om deras sekretesspolicy.

Typ: Identifierbar

Var: Kanada

Vem: SMART Technologies ULC

Roll: Tillverkare

Information/Syfte: Nödvändig kontoinformation: organisationsnamn, e-post-adress,

subscriptions. Required order information: product, quantity, price and tax, delivery. Required admin portal information for license provisioning: licenses and activations, teachers', and admins' first and last names (can provide non-PII version to comply with GDPR) and e-mail address, and class names (can be non-PII version to comply with GDPR).

SLS Terms

GDPR - EC Adequacy Decision

Typ: Identifiable

Where: Canada

Who: Blue Ocean Contact Centers, Inc.

Role: Support

Data/Purpose: Optional. Blue Ocean is a subcontractor providing live (telephone, e-mail, and web) support. Information collected includes organization name, caller name (can use company title only if preferred for GDPR reasons), e-mail (can provide non-PII version to comply with GDPR), title, phone, address and a description of the issue and any shared details to help solve the problem. Calls are recorded.

Blue Ocean Privacy

GDPR - EC Adequacy Decision

Typ: Identifiable

Where: USA/Germany

Who: Amazon Web Services, Inc..

Role: Processing, Back Office

Data/Purpose: Required for product infrastructure including the hosting of support call recordings.

AWS Privacy

befattning, telefonnummer, adress, återförsäljare, nuvarande prenumerationer.

Nödvändig orderinformation: produkt, antal, pris och skatt, leverans. Nödvändig administrativportalinformation för licenseringsutgivande: licens och aktivering, lärares och administratörers för- och efternamn (kan ge ut icke-PII versioner i efterlevnadssyfte med GDPR) och e-post-adresser and klassnamn (kan vara icke-PII versioner i efterlevnadssyfte med GDPR).

SLS-villkor

GDPR – EC Adequacy Decision

Typ: Identifierbar

Var: Kanada

Vem: Blue Ocean Contact Centers, Inc.

Roll: Support

Information/Syfte: Valfri. Blue Ocean är en underleverantör som bistar med live (telefon, e-post och på internet) support. Insamlade uppgifter inkluderar organisationsnamn, namn på den som ringer upp (företagsbefattning kan användas i GDPR-syfte), e-post (kan ge ut icke-PII versioner i efterlevnadssyfte med GDPR), befattning, telefonnummer, adress och en beskrivning av problemet och de detaljer som delas i syfte att lösa problemet. Samtalen spelas in.

Blue Ocean sekretess

GDPR – EC Adequacy Decision

Typ: Identifierbar

Var: USA/Tyskland

Vem: Amazon Web Services, Inc..

Roll: Behandling, back office

Information/Syfte: Nödvändig för produktinfrastruktur, inklusive hosting av samtal med supporten.

AWS sekretess

AWS GDPR

Typ: Identifiable

Where: USA

Who: Google, LLC.

Role: Processing, Back Office

Data/Purpose: Optional. Only used for processing of support forms. Google Forms are used when a purchaser is engaged with our Field Services (i.e., onsite support).

Google Privacy
Google GDPR

Typ: Identifiable

Where: USA

Who: Microsoft, Inc.

Role: Processing, Back Office

Data/Purpose: Required for our enterprise resource planning (ERP) system, which is software to manage the day-to-day business activities such as accounting, procurement, project management and supply chain operations, as well as our e-mail, PowerBI® (data visitation) and SharePoint® (document management), as well as all the other standard Microsoft Office software titles, like Word, Excel, etc.

Microsoft Privacy
Microsoft GDPR

Typ: Identifiable

Where: USA

Who: BigCommerce, Inc.

Role: Ordering

Data/Purpose: Optional. Only used when a customer purchases through our e-commerce store: customer name, e-mail, title, phone, address, product, or service purchased and whether payment is received.

AWS GDPR

Typ: Identifierbar

Var: USA

Vem: Google, LLC.

Roll: Behandling, back office

Information/Syfte: Valfri. Används enbart för hantering av supportformulär. Google Forms används när en köpare är engagerad med våra Field Services dvs. support på plats.

Google sekretess
Google GDPR

Typ: Identifierbar

Var: USA

Vem: Google, LLC.

Roll: Behandling, back office

Information/Syfte: Nödvändig för vårt enterprise resource planning system (ERP), vilket består av mjukvara som handhar dagliga affärshändelser såsom redovisning, anskaffning, projektledning, vår e-post PowerBI® (data visitation) och SharePoint® (dokumenthantering), samt alla andra standardprogram i Microsoft Office-suiten, som Word, Excel och så vidare.

Microsoft sekretess
Microsoft GDPR

Typ: Identifierbar

Var: USA

Vem: BigCommerce, Inc.

Roll: Ordrrar

Information/Syfte: Valfri. Används enbart när en kund handlar genom vår e-handelsfunktion: kundens namn, e-post adress, befattning, telefonnummer, adress, produkt eller

BigCommerce Privacy BigCommerce GDPR	service som köpts samt om betalning mottagits.
Typ: Identifiable	BigCommerce sekretess BigCommerce GDPR
	Typ: Identifierbar
Where: USA	Var: USA
Who: Stripe, Inc. and Stripe Payments Europe, Ltd.	Vem: Stripe, Inc. and Stripe Payments Europe, Ltd.
Role: Ordering	Roll: Ordrar
Data/Purpose: Optional. Only used when a customer purchases through our e-commerce store using a credit card: customer name, e-mail, title, phone, address, product, or service purchased, credit card details. Residents of the European Economic Area (EEA), the UK and Switzerland. The entity responsible for the collection and processing of credit card personal data for residents of the EEA, the UK and Switzerland is Stripe Payments Europe, Ltd., a company incorporated in Ireland and with offices at 1 Grand Canal Street Lower, Grand Canal Dock, Dublin. To exercise your rights, the Data Protection Officer may be contacted via dpo@stripe.com .	Information/Syfte: Valfri. Används enbart när en kund handlar genom vår e-handelsfunktion med kreditkort: kundens namn, e-post adress, befattning, telefonnummer, adress, produkt eller service som köpts, kreditkortsdetaljer. Innevärdare i EES, Storbritannien och Schweiz. Den part som har ansvaret för insamling och behandling av personuppgifter från kreditkort för innevärdare i EES, Storbritannien och Schweiz är Stripe Payments Europe, Ltd., ett företag registrerat i Irland med kontorsadress 1 Grand Canal Street Lower, Grand Canal Dock, Dublin. För att tillvarata dina rättigheter, dataskyddsombud kan nås på dpo@stripe.com
Stripe Privacy Stripe GDPR	Stripe sekretess Stripe GDPR
Typ: Identifiable	Typ: Identifierbar
Where: USA	Var: USA
Who: Salesforce.com, Inc.	Vem: Salesforce.com, Inc.
Role: Ordering, Marketing, Channel Support	Roll: Ordrar, marknadsföring, support för kanaler
Data/Purpose: Required order information (product, quantity, price and tax, delivery). Required for our customer relationship management (CRM). Required to allow our authorized distributors and resellers to work together with SMART. Basic customer and purchase information is shared between SMART and its authorized distributors and resellers.	Information/Syfte: Nödvändig orderinformation (product, antal, pris och skatt, leverans). Nödvändig för vår customer relationship manager (CRM). Nödvändig för att tillåta våra auktoriserade distributörer och återförsäljare att arbeta tillsammans med SMART. Grundläggande kundinformation och information om köp delas mellan SMART och dess auktoriserade distributörer och återförsäljare.
Salesforce Privacy	

Salesforce GDPR

Typ: Identifiable

Where: USA

Who: HubSpot, Inc.

Role: Marketing

Data/Purpose: Optional. We use HubSpot, which is a customer relationship management (CRM), for individuals that have expressly opted in to receive certain communications, such as marketing, training, news, and offers from us.

Hubspot Privacy
Hubspot GDPR

Typ: Identifiable.

Where: USA

Who: Mixpanel, Inc.

Role: Monitoring

Data/Purpose: Required for product improvement and service monitoring. Mixpanel allows us to analyse how our de-identified users interact with Notebook. It is designed to identify trends, understand common aggregated usage behaviour, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime.

Mixpanel Privacy
Mixpanel GDPR

Typ: Pseudonymized.

Where: USA

Who: Gainsight, Inc.

Salesforce sekretess
Salesforce GDPR

Typ: Identifierbar

Var: USA

Vem: HubSport, Inc.

Roll: Marknadsföring

Information/Syfte: Valfri. Vi använder HubSport, ett customer relationship management-verktyg (CRM), för individer som har uttryckligen godkänt att de önskar motta viss information, såsom marknadsföring, träning, nyheter och erbjudanden från oss.

Hubspot sekretess
Hubspot GDPR

Typ: Identifierbar

Var: USA

Vem: Mixpanel, Inc.

Roll: Övervakning

Information/Syfte: Nödvändig för produktutförbättring och övervakning av tjänst. Mixpanel tillåter oss att analysera hur våra avidentifierade användare interagerar med Notebook. Det är designat för att identifiera trender, förstå sammanslagen aggregerat användarbeteende och hjälper oss att ta bättre beslut kring hur användarvänligheten och funktioner i vår produkt kan förbättras. Denna information används även för att mäta hur lång tid det tar för våra servrar att slutföra handlingar så som öppna filer, vilket hjälper oss mäta tjänstens status och up/downtime.

Mixpanel sekretess
Mixpanel GDPR

Typ: Pseudomiserad

Var: USA

Vem: Gainsight, Inc.

Role: Marketing

Data/Purpose: Applicable only to USA customers. We use Gainsight, which is a customer relationship management (CRM) tool, for e-mail (name, e-mail address, company information) marketing to individuals and organizations.

Gainsight Privacy

Typ: Identifiable.

Roll: Marknadsföring

Information/Syfte: Gäller bara för kunder baserade i USA. Vi använder Gainsight, ett customer relationship management- verktyg (CRM), för marknadsföring via e-post (namn, e-post adress, företagsinformation) till individer och organisationer.

Gainsight sekretess

Typ: Identifierbar

Footnotes

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(3) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Fotnoter

(1) Om uppgiftsutföraren är ett personuppgiftsbiträde som omfattas av förordning (EU) 2016/679 och som agerar på uppdrag av en unionsinstitution eller ett unionsorgan som personuppgiftsansvarig, säkerställer användningen av dessa klausuler vid anlitande av ett annat personuppgiftsbiträde (som underentreprenör) som inte omfattas av förordning (EU) 2016/679 även överensstämmelse med artikel 29.4 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39), i den utsträckning som dessa klausuler och de skyldigheter i fråga om uppgiftsskydd som fastställs i avtalet eller en annan rättsakt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i enlighet med artikel 29.3 i förordning (EU) 2018/1725 har samordnats. Detta kommer särskilt att vara fallet om den personuppgiftsansvarige och personuppgiftsbiträdet använder de standardavtalsklausuler som ingår i beslut 2021/915.

(2) Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till avtalet. Om uppgiftsföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

(3) När det gäller konsekvenserna av sådana lagar och förfaranden för efterlevnaden av dessa klausuler kan olika aspekter anses utgöra en del av den övergripande bedömningen. Sådana aspekter kan omfatta relevant och dokumenterad praktisk erfarenhet av tidigare begäranden om utlämning av uppgifter från offentliga myndigheter, eller avsaknad av sådana begäranden, som täcker en tillräckligt representativ tidsram. Detta gäller särskilt interna register eller annan dokumentation som upprättats kontinuerligt i enlighet med tillbörlig aktsamhet och som godkänts på ledningsnivå, under förutsättning att denna information kan delas med tredje parter på ett lagligt sätt. Om denna praktiska erfarenhet används som grund för slutsatsen att uppgiftsinföraren inte kommer att hindras från att uppfylla kraven i dessa klausuler måste den stödjas av andra relevanta, objektiva aspekter, och parterna måste noggrant överväga huruvida dessa aspekter tillsammans har tillräckligt stor vikt, vad gäller deras tillförlitlighet och representativitet, för att underbygga denna slutsats. Parterna måste i synnerhet ta hänsyn till huruvida deras praktiska erfarenhet bekräftas och inte motsägs av offentligt tillgänglig eller på annat sätt åtkomlig och tillförlitlig information om förekomst eller avsaknad av begäranden inom samma sektor och/eller av tillämpningen av lagstiftningen i praktiken, t.ex. rättspraxis och rapporter från oberoende tillsynsorgan.