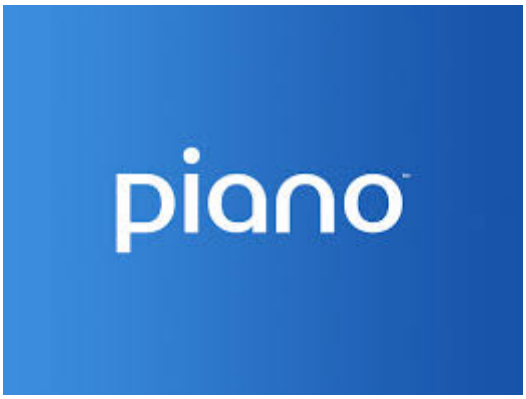
BINDING CORPORATE RULES

of

PIANO GROUP



acting as a controller (BCR-C)

pursuant to the Article 47 GDPR

XX 2021

TABLE OF CONTENTS

Preamble	3
1 Subject matter	4
2 BCR membership and liability	4
3 Binding nature of BCRs	5
4 Third party beneficiary clause	6
5 Cross-Border Processing	7
6 Compliant mechanism	8
7 Data protection safeguards	8
8 Supplementary measures	14
9 Final provisions	16

Terms beginning with capital letters and definitions used in these BCRs have meaning prescribed to them in Annex A (Definitions) hereto.

WHEREAS:

(A) Piano Group wishes to comply with the GDPR;

(B) Piano Group decided to adopt these BCR primarily in order to ensure compliance with GDPR in situations where Piano Group processes personal on a cross-border basis as a controller;

(C) The main establishment of Piano Group in the EU as regards processing personal data is historically located in Slovakia making the Slovak SA the lead SA of Piano Group entitled to approve these BCRs;

(D) The list of BCR Members (Annex B hereto) may change from time to time, without the need of updating these BCRs as stems further from below;

(E) These BCRs also contain the Group Data Processing Agreement which is part of membership in these BCRs (Annex C hereto);

THEREFORE, PIANO GROUP ADOPTS THESE BCR IN THE FOLLOWING WORDING:

1 SUBJECT MATTER

1.1 **Material scope**. These BCRs apply to where Piano Group (BCR Members) act as joint controllers for joint purposes of processing, as is described in more detail in Section 5 below (the „**Cross-Border Processing**“).

1.2 **Geographical scope**. These BCRs apply to Cross-Border Processing from the EEA to the US or other third countries where BCR Members are established as per Annex B hereto as well as to: (i) any subsequent processing of personal data by BCR Members in such third countries, and; (ii) any subsequent onward transfers to or sub-processing of non–Piano Group (external) entities.

1.3 These BCRs do not apply to all processing of personal data within Piano Group irrespective of the origin of the personal data, but only apply to joint-controller activities as per Section 1.1 and Section 1.2 above, where such personal data originate or is exported from the BCR Members established in the EEA.

1.4 If the Applicable Data Protection Law requires higher level of protection of personal data than the GDPR or these BCRs, it will take precedence over these BCR. If the Applicable Data Protection law requires lower level of protection of personal data than these BCRs, Piano Group will apply these BCRs.

2 BCR MEMBERSHIP AND LIABILITY

2.1 Any Piano Group entity becomes the BCR Member by signing the declaration in Annex B hereto.

2.2 First BCR Members are listed in Annex B hereto. List of BCR Members may change from time to time without the need to re-apply for approval of these BCRs provided that Section 2.3 below is complied with. Piano Group entity may withdraw the membership in BCRs only with the prior written consent of the CEO, after consulting the DPO.

2.3 List of all BCR Members is internally kept, maintained and updated by the DPO. Consolidated list of all BCR Members must be published and regularly updated at the BCR Homepage. By the end of each January, the DPO shall communicate the consolidated list of all BCR Members effective as of December 31st of the previous year to the Slovak SA by email (statny.dozor@pdp.sk) or by post and shall keep evidence of such notification in DPO File (as defined below).

2.4 By signing the declaration in Annex B hereto, each BCR Member agrees to co-operate with, to accept to be audited by the competent SAs and to comply with the advice of these competent SAs on any issue related to these BCRs.

2.5 Each BCR Member is liable for any damage it causes by breaching these BCRs.

2.6 Notwithstanding the above Section 2.5 and since the main headquarters of Piano Group is not located in the EU, Piano Slovakia is appointed as the BCR Member with delegated responsibilities pursuant Article 47 (2) (f) of the GDPR meaning Piano Slovakia accepts:

(a) the liability for any breaches of these BCRs by any BCR Member not established in the EU including the liability to pay compensation for any material or non-material damages resulting from the violation of the BCRs by such BCR Members while Piano Slovakia shall be exempt from that liability, in whole or in part, only if it proves that that BCR Member is not responsible for the event giving rise to the damage;

(b) that in case BCR Member not established in the EU violates these BCRs, the courts or other competent SA in the EU will have jurisdiction over the dispute and the data subject

will have the rights and remedies against Piano Slovakia as if the violation had been caused by Piano Slovakia instead of the BCR Member outside the EU;

(c) that the burden of proof to demonstrate that the BCR Member outside the EU is not liable for any violation of BCRs which has resulted in the data subject claiming damages will lie on Piano Slovakia, not on the data subject; and

(d) to take the necessary action to remedy the acts of other BCR Members outside of the EU.

2.7 By becoming BCR Member each BCR Member concludes the Group Data Processing Agreement (Annex C).

2.8 Breach of these BCRs by Piano Group personnel may be assessed as: (i) violation of the working discipline; (ii) violation of a contractual obligation to respect and comply with these BCRs; (iii) violation of a statutory obligation to respect and comply with internal polices, codes or procedures. Such breach may lead to: (i) termination of the employment or other contract; (ii) incurring damages by Piano Group or third parties; and subsequently (iii) claiming incurred damages by Piano from such personnel of Piano Group.

3 BINDING NATURE OF BCRS

3.1 By signing the declaration in Annex B, these BCRs become binding to such BCR Member and such BCR Member may rely on these BCRs as the appropriate safeguards for the Cross-Border Processing.

3.2 These BCRs are legally binding to all BCR Members both internally and externally. Each BCR Member including their employees, directors and staff must respect and comply with these BCRs. These BCR are legally binding to BCR Members and its personnel, staff and directors[1] on the basis that these BCRs:

(a) represent legally binding instruction of Piano Software, Inc. (Philadelphia, US) to other BCR Members pursuant to the Article 28 and 29 of the GDPR on as to how personal data are handled within Piano Group;

(b) represent legally binding internal data protection policy of Piano Group pursuant to the Article 32 (4) of the GDPR;

(c) are contractually accepted by BCR Members by signing the declaration in Annex B hereto.

3.3 These BCRs as well as the most up to date list of BCR Members shall always be published at the BCR Homepage. These BCRs must be always easily accessible to personnel, staff and directors of BCR Members to whom BCRs are addressed to. If required under local law (e.g. employment law), BCR Members shall undertake any and all additional steps for these BCRs to be legally binding and enforceable against its personnel, staff and directors. If any part or provision of these BCRs turns out to be non-binding or non-enforceable against any personnel, staff or director or the BCR Member itself, the affected BCR Member must immediately report this to CEO and DPO.

3.4 Every BCR Member shall be responsible to demonstrate compliance with these BCRs upon request of the CEO, DPO or the SA.

[1] Irrespective of whether their cooperation is of business, civil, volunteer or employment nature.

4 THIRD-PARTY BENEFICIARY CLAUSE

4.1 Piano Group explicitly warrants and agrees that data subjects who are subject to the Cross-Border Processing whatever their nationality or residence can, as a third-party beneficiary, enforce below listed provisions of these BCRs and any data subject rights stemming from the GDPR or the Applicable Data Protection Law against any BCR Member including: right to access (Article 15 GDPR); right to rectification (Article 16 GDPR); right to erasure (Article 17 GDPR); right to restriction (Article 18 GDPR); right to be notified about rectification or erasure of personal data or restriction of processing (Article 19 GDPR); right to data portability (Article 20 GDPR); right to object (Article 21 GDPR); right not to be subject to the automated decision making including profiling (Article 22 GDPR).

4.2 This third-party beneficiary clause applies specifically to the following provisions of these BCRs: 2.4, 2.5, 2.6, 2.7, 3, 4 and 7. In addition, data subjects have right to:

(a) lodge a complaint against any BCR Member pursuant to Section 6 below;

(b) lodge a complaint against any BCR Member before the competent SA pursuant to the Article 77 of the GDPR;

(c) effective judicial remedy before the competent EU court pursuant to the Article 79 of the GDPR;

(d) judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCRs;

(e) rely on these BCRs even if the local law prevents them do so or invalidates these BCRs.

4.3 Every data subject that is subject to the Cross-Border Processing has right to lodge complaint against any BCR Member with competent SA, in particular in the EU Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes these BCRs or the Applicable Data Protection Laws.[2]

4.4 Every data subject that is subject to the Cross-Border Processing has right to enforce these BCRs against any BCR Member before the courts of the EU Member State where such BCR Member is established. Alternatively, such proceedings may be brought before the courts of the EU Member State where the data subject has his or her habitual residence.[3]

4.5 In relation to the Cross-Border Processing, Piano Group warrants that all concerned data subjects will be provided with the information as required by Articles 13 GDPR[4] and Article 14 GDPR in

[2] For more details, see Article 77 GDPR: "**Right to lodge a complaint with a supervisory authority**. (1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. (2) The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78."

[3] For more details, see Article 78 GDPR: „**Right to an effective judicial remedy against a controller or processor**. (1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. (2) Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."

[4] This includes the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients

the Privacy Policy. In addition, the Privacy Policy shall include a link to published BCRs allowing data subject to familiarize themselves with the wording of these BCRs.

4.6 Every data subject that is subject to the Cross-Border Processing must have an easy access to these BCRs. In addition to publishing BCRs on the BCR Homepage, Piano Group will distribute BCRs internally to its staff (e.g. via intranet) and provide the latest version of BCRs to data subject concerned upon their request.

4.7 Any request made directly against BCR Member under this Section 4 or any motion to enforce third-party beneficiary clause can be made via the complaint mechanism under Section 6 below.

4.8 To ensure the binding nature of this Section 4 towards 3rd party beneficiaries, all BCR Members explicitly confirm that by accession to these BCRs and by concluding the Group Data Processing Agreement, the possibility of 3rd parties to bindingly enforce 3rd party beneficiary clauses herein stems both from: (i) universal declarations provided by all BCR Members in this Section 4 as well as for; (ii) contractual arrangement included in the Group Data Processing Agreement.

5 CROSS-BORDER PROCESSING

5.1 **Transfers or set of transfers**. As a controller, Piano Group processes personal data for its own purposes of processing described in Section 5 of the Group Data Processing Agreement. Such purposes should cover all processing operations by Piano Group outside the processing under the DPA. Should these purposes of processing change, Piano Group entities shall update the Group Data Processing Agreement immediately. Change of the Group Data Processing Agreement shall not require or be regarded as change of these BCRs.

5.2 **Categories of personal data**. Any personal data that Piano Group needs to, is entitled to or is required to process in order to fulfill the purposes of processing mentioned in Section 5 of the Group Data Processing Agreement.

5.3 **Type of processing**. Processing is conducted by both automated / electronic and manual means.

5.4 **Purposes of processing**. Purposes of processing mentioned in Section 5 of the Group Data Processing Agreement.

5.5 **Type of data subjects affected**. Any type of data subject whose personal data need to processed in order to fulfil Piano's purposes of processing including employees, directors and staff of Piano Group, representatives or contact persons of Piano's suppliers or business partners, visitors of Piano's websites or social media profiles, as is described in more details in Section 14 of the Group Data Processing Agreement.

5.6 **Third countries**. Piano Group processes personal data within the EU, US and other third counties where BCR Members are currently located, as stems from Annex B hereto.

---

of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. In addition: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. In line Article 13 (4) GDPR, the above information does not need to provided where and insofar as the data subject already has the information.

5.7 **Group Data Processing Agreement**. Piano Software, Inc. concluded the Group Data Processing Agreement with all other Piano Group entities acting as joint controllers to jointly process personal data for its own purposes in line with Art. 26 of the GDPR.

6 COMPLAINT MECHANISM

6.1 Data subjects which are subject to the Cross-Border Processing have right to lodge a complaint against any BCR Member in matters related to the Cross-Border Processing, violation of these BCRs, enforcing their rights or relying on third-party beneficiary clauses as per Section 4 above.

6.2 Complaint can be made using the Complaint Form as prescribed by in Annex D. The Complaint Form should be always available in an online form at the BCR Homepage. Data subjects are however free to draft any complaint themselves without using the Complaint Form as a basis. Any complaint should be addressed to:

(i) dpo@piano.io when made electronically by email; or

(ii) Piano Group DPO, Piano Software, s.r.o., Štefánikova 14, Bratislava 811 05, Slovakia when made in writing by post;

(iii) contact details of any BCR Member mentioned in the Annex B.

6.3 Should any compliant be received by any BCR Member, such BCR Member is obliged to forward such compliant to the DPO without undue delay.

6.4 All complaints must be dealt with by Piano without undue delay, at the latest within 1-month from the receipt of the complaint. Taking into account the complexity and number of the requests, that 1-month period may be extended at maximum by further 2 months, in which case the data subject should be informed accordingly within the original 1-month period from the receipt of the complaint.

6.5 DPO is responsible for handling complaints. DPO is entitled to delegate responding, preparing a draft answer to the complaint or gathering necessary information to another department or person within Piano Group.

6.6 DPO is responsible for keeping a record of complaints received under these BCRs in electronic form. The record contains the following information: name, surname and address of a complainant, date of the receipt of a complaint, concise summary of the complaint, response to a complaint and the date of the dispatch of the response to a complaint.

6.7 Response to the complaint must take into the account specifics of the given situation and data subject. Unless these specifics require otherwise, in general, the response to the complaint is either: (i) rejection of the complaint; or (ii) considering the complaint justified.

7 DATA PROTECTION SAFEGUARDS

7.1 **Training program**. Employees, directors and staff of Piano Group who have permanent or regular access to personal data or are involved in the collection of data or in the development of tools used to process personal data shall be regularly attend appropriate training on these BCRs, data protection and security. DPO shall develop and oversee a suitable training program at Piano Group. The training program shall consist at least of one monthly awareness training and one annual assessment.

7.2 **Audit program**. Piano Group shall conduct regular data protection audits to ensure verification of compliance with these BCRs, including audit of all relevant IT systems, databases, security

policies and, if applicable, the physical record systems of Piano Group. Such audits may cover wider overall data protection compliance of Piano Group where verification of compliance with these BCRs is only part of the audit, or such audits can be focused solely on these BCRs. In addition to regular audits, Piano Group shall also conduct ad hoc data protection audits in case of need to address any operational compliance concerns including personal data breach. The regular audits shall be:

(a) conducted on annual basis;

(b) conducted by either internal or external data protection auditors;

(c) covering all aspects of these BCRs including methods of ensuring that corrective actions will take place.

7.3 Results of such audits shall be formulated in an audit report with key findings and recommendations. Audit report shall be communicated to the CEO, DPO and the management of Piano Group.

7.4 All audit reports are archived and stored by the DPO in the DPO File for a period of at least 3 years.

7.5 SA can have access to such audit reports covering these BCRs upon request.

7.6 Piano Group hereby agrees and warrants that the competent SAs is authorized to conduct audit or inspection of any BCR Member. Each BCR Member is obliged to cooperate with the competent SAs.

7.7 **DPO**. Piano Group has a long-term commitment to have appointed the DPO irrespective of whether requirements of Article 37 GDPR are met or not. The DPO shall:

(a) be appointed directly by Piano Slovakia;

(b) notified to the Slovak SA;

(c) monitor Piano Group's compliance with these BCRs;

(d) keep, maintain and update the list of all BCR Members including storing the BCR Members' declarations pursuant to the Annex B hereto;

(e) liaise with the Slovak SA and SA concerned as regards approval, changes, updates or any communication regarding these BCRs;

(f) oversee the audit program under point 7.2 above;

(g) oversee the training program under point 7.1 above;

(h) handle complaint mechanism under point 6 above;

(i) evaluate local law of the third countries pursuant to the point 7.9 below;

(j) report to the competent SAs any problems with local law of third countries pursuant to the point 7.10 below;

(k) be assisted by a team of DPEs as stems from point 7.8 below;

(l) enjoy the highest management support from Piano Group for fulfilling of tasks under these BCRs;

(m) comply with additional tasks and responsibilities under Internal Policies.

7.8 **Internal network**. Piano Group has established the following internal network of selected roles (CEO, DPO, DPEs and other personnel) in order to comply with these Applicable Data Protection Laws, BCRs and Internal Policies:

Roles	General responsibilities
Chief Executive Officer ("**CEO**")	▪ Manages data protection & information security; ▪ Is ultimately responsible for data protection compliance; ▪ Decides on escalations; ▪ Approves updates of this policy and BCRs; ▪ Appoints DPO, ISM and DPEs via this Group Policy; ▪ Maintains adequate budget for security and data protection compliance;
DPO	▪ Monitors overall data protection compliance of Piano Software Group; ▪ Reports to the CEO; ▪ Provides information, support and advice to the highest management of Piano Software Group on data protection issues; ▪ Ensures other internal policies at Piano Software Group are compliant with BCRs; ▪ Maintains the DPO File; ▪ Raises awareness and trains personnel of Piano Software Group in the area of the data protection; ▪ Acts as a contact point for any SA or data subjects;
Deputy DPO	▪ Substitutes DPO in case of DPO's absence; ▪ Substitutes DPO in case a risk of DPO being in a conflict-of-interest situation;
ISM	▪ Monitors information security agenda at Piano Software Group; ▪ Reports to the CEO as regards information security; ▪ Supports DPO in fulfilling its tasks under this policy and BCRs; ▪ Raises awareness and trains personnel of Piano Software Group on the cybersecurity or information security;
Data Protection Executive („**DPE**")	▪ Supports DPO in fulfilling its tasks; ▪ Complies with DPO's instructions;
Internal recipients of personal data ("**Employees**")	▪ Process personal data in line with these BCRs, internal policies at Piano Software Group and DPO's instructions.

Exact processes and more detailed definition of tasks and responsibilities must be defined and described in the Group Policy. Such internal network is group-wide and is independent from any other organizational structure in place. At Piano Group, a team of DPEs reports to the DPO while the DPO can issue a binding instructing to DPEs in any data protection compliance aspect. CEO remains the ultimate decision-maker while the DPO retains its independent status by being afforded to record and store his differing opinions. In addition, Piano Group adopted the escalation process under which DPEs can challenge DPOs instructions before the CEO. The DPO: (i) is the main contact point for SAs; (ii) is responsible for updating the Privacy Policy; (iii) handles data subject requests and complaints under these BCRs; (iv) coordinates regular data protection audits at Piano Group; (v) closely cooperates with ISM; (vi) advises on the data protection impact assessments, and fulfils other tasks. This internal network shall support DPO in fulfilling its tasks also under these BCRs.

7.9 **Local law**. Each BCR Member must continuously monitor the existing and future local law of the country where such BCR Member is established, irrespective of whether established in the EEA or third country. The aim of such monitoring is to analyze whether: (a) the local law is not contrary to the GDPR; (b) whether any local law would not have a substantial adverse effect on the guarantees provided by these BCRs; and generally (c) whether these BCRs will be complied with by BCR Member when complying with such local law. Piano shall comply with the local law, however, if the BCR Member has reasons to believe that the local law prevents the BCR Member to comply with these BCRs, is contrary to GDPR, has substantial effect on the guarantees

provided herein or compliance with would lead to not complying with these BCRs, **the affected BCR Member must immediately report this to the Piano Slovakia and the DPO**. Any legally binding request from public authorities to access or actual access to personal data processed by Piano Group must be immediately notified to Piano Slovakia and the DPO. Following the internal reporting of the problematic local law in third country pursuant to this Section 7.9, Piano Group shall make an individual case-by-case assessment of the situation pursuant to the Section 8 below.

7.10 **Reporting to competent SAs**. Where any legal requirement a BCR Member is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by these BCRs, the problem should be reported to and consulted with the Slovak SA and other competent SAs (if any)[5] by the DPO. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. In such a case, the competent SAs should be informed by the DPO about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). If in specific cases the suspension and/or notification are prohibited, the BCR Member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so. If, in the above cases, despite having used its best efforts, the Piano Group is not in a position to notify the competent SAs, the Piano Group commits to annually provide general information on the requests it received to the competent SA (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.), if such requests where received in the previous year.

7.11 **Proportionality.** Without regard to the above, in any case, transfers of personal data by the Piano Group to any public authority **cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society**.

7.12 **Records of processing activities**. Piano Group shall maintain controller's records of processing activities in writing (including electronic form) which shall be made available to the SA upon request. Records of controller processing activities shall include at least the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards where applicable; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures adopted. As prerequisite for complying with these BCRs, Piano Group shall play special emphasis on identifying and listing in such records all cross-border transfers of personal data.

7.13 **DPIA and prior consultation**. Where required, Piano Group shall conduct DPIA covering / on behalf of all BCR Members and/or taking into the account the Cross-Border Processing. Where the DPIA indicates that the processing would result in a high risk in the absence of measures taken by Piano to mitigate the risk, the Slovak SA should be consulted prior to such processing..

[5] By default, the Slovak SA is always competent for reporting and consulting under this Sectin 7.10. However, Piano Group shall always assess whether additional competent SAs should not be reported to as well, as per Article 55 and Article 56 GDPR. For example, should the issue be more pressing for particular BCR Member or data subject in particular EU Member State, competent SA in such EU Member States should be reported and consulted as well. On the other hand, if there is no clear connection with jurisdiction of the particular EU BCR Member, its SA does not need to be notified or reported under Section 7.10.

7.14 **Data protection by design**. All BCR Members shall implement appropriate technical and organizational measures designed to implement data protection principles and to facilitate compliance with the requirements set up by the BCRs in practice. For any aspect of compliance with these BCRs or with data protection principles the following principles shall be considered:

(a) proactive not reactive approach;

(b) data protection being the default setting;

(c) data protection being embedded into design;

(d) full lifecycle protection (end-to-end security);

(e) visibility and transparency;

(f) respect for user privacy.

7.15 The DPO shall always evaluate the above principles in the given situation in case anyone from Piano Group's personnel asks the following question: „***What impact will that have on guarantees provided by BCRs or data protection principles?***" (the "**Triggering Question**"). The training program should educate personnel to spot when to ask the Triggering Question, mainly before any new process, decision or project at Piano Group that may have impact on the guarantees provided by these BCRs or overall level of data protection at Piano Group. Nothing in Internal Policies shall limit the right of Piano Group's personnel to ask the Triggering Question at any time. Whenever the Triggering Question is asked, the DPO shall be asked for advice. DPO documents all Triggering Questions, advice given, and measures implemented as a result of it.

7.16 **Data protection by default**. All BCR Members shall implement appropriate technical and organizational measures designed to implement data protection by default to only process personal data in an extent that is necessary for the given purpose of processing. This obligation applies to the amount of personal data collected, the extent of their processing, the duration of their storage and their availability. In particular, such measures shall ensure that personal data are not normally accessible to an unlimited number of persons at Piano Group.

7.17 **Data protection principles**. BCR Members shall observe the basic data protection principles, in particular:

(a) transparency, fairness and lawfulness under Article 5 (1) (a) GDPR;

rule: *Piano Group will always inform data subjects transparently about processing their personal data in its Privacy Policy; and*

rule: *Piano Group will only process personal data fairly and based on sufficient legal basis;*

(b) purpose limitation under Article 5 (1) (b) GDPR;

rule: *Piano Group will only collect personal data for specified, explicit and legitimate purpose of processing;*

(c) data minimization under Article 5 (1) (c) GDPR;

rule: *Piano Group will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes of processing;*

(d) data accuracy under Article 5 (1) (d) GDPR;

rule: *Piano Group will only process accurate and up to date personal data;*

(e) limited storage periods under Article 5 (1) (e) GDPR;

rule: *Piano Group will not keep personal data in a form permitting identification of data subjects for longer than is necessary for the purposes of processing;*

(f) integrity and confidentiality under Article 5 (1) (f) GDPR; and

rule: *Piano Group will adopt adequate security measures to protect personal data;*

(g) accountability under Article 5 (2) GDPR;

rule: *Piano Group is responsible for compliance with these basic principles and shall be able to demonstrate compliance with them at any time not only by internal policies and procedures but by actual steps, actions and measures;*

as stems in more detail from these BCRs.

7.18 **Legal bases**. BCR Members shall only process personal data based on one or more legal bases under Article 6 GDPR. Where special categories of personal data are processed, conditions under Article 9 GDPR must be complied with in addition to Article 6 GDPR. The specific legal basis relied upon by BCR Members are specified in the Group Data Processing Agreement.

7.19 **Processors and transfers**. According to the Group Data Processing Agreement, Piano Software, Inc. is the only BCR Member authorized to conclude data processing agreement pursuant to the Articles 28 or 26 of the GDPR with third parties (and hence transfer personal data outside the Piano Group) also on behalf and for the benefit of the whole Piano Group. Therefore, if any BCR Member intends to use other processors, sub-processor or joint controllers for processing of personal data covered by the Group Data Processing Agreement, it shall only do so with explicit prior consent from Piano Software, Inc. In any other cases, BCR Members shall notify DPO about using other processors, sub-processor or joint controllers and must conclude data processing agreements pursuant to the Articles 28 or 26 of the GDPR, if required. Consent of Piano Software, Inc. appointment of processor or transfer pursuant to this point must not be granted as regards Cross-Border Processing, where no adequate protection is provided according to Articles 45 to 48 GDPR and no derogation according to Article 49 GDPR applies.

7.20 **Security**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each BCR Member shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

7.21 **Breaches**. Any personal data breach pursuant to the Article 4 (12) of the GDPR must be immediately (without undue delay) notified by any BCR Member or any Piano Group personnel to the DPO. Any personal data breaches at Piano Group are evaluated, documented and further reported by the DPO. The template for personal data breach documentation that shall be used by BCR Members to document any personal data breach is also included in Annex E of these BCRs. Any personal data breach documentation shall be made available to the competent SA upon request in line with Article 33 and 34 of the GDPR. The DPO is responsible for notification of:

(a) the SA that should be notified about the data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay;

(b) the data subjects when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The notification should be sent without undue delay in clear and plain language and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3) of the GDPR.

7.22 **Onward transfers**. Any onward transfer of personal data to controllers or processors other than BCR Members which are established in third countries (i.e. outside EEA) is prohibited, unless following conditions:

(a) such onward transfer is approved in accordance with Section 7.20 above;

(b) if the recipient is data processor or joint controller, obligations under Articles 26 and 28 GDPR are fully complied with by Piano Group;

(c) adequate protection is provided in accordance with Articles 45 to 48 GDPR or under derogation according to Article 49 GDPR.

8 SUPPLEMENTARY MEASURES

8.1 To facilitate effectiveness of the third country's local law monitoring (Section 7.9 above) and subsequent decisions taken, Piano Group adopted the following process:

- **1st step: Assessment followed by decision;**
- **2nd step: Identifying supplementary measures;**
- **3rd step: Procedural steps; and**
- **4th step: Re-evaluation**,

as described in more detail below.

8.2 **Assessment**. Following the notification or reporting of potentially problematic 3rd country local legislation[6] under Section 7.9 above, Piano Group shall make a more detailed legal and practical assessment of the situation on a case-by-case basis. Where necessary, this assessment should be made with the involvement of local importer and/or local legal counsel. Within such assessment, Piano Group shall consider the legal or official wording of the local law as well as the known practices in such 3rd country. In particular, Piano Group shall assess whether one of the following applies:

i. legislation in the 3rd country formally meeting EU standards is manifestly not applied/complied with in practice;

ii. there are practices incompatible with the commitments under these BCRs where relevant legislation in the 3rd country is lacking;

iii. transferred personal data or importer in 3rd country fall or might fall within the scope of problematic legislation.

8.3 The assessment above and subsequent decisions below shall be documented and kept by the DPO in DPO File for any inspection by competent SAs. Among others, the assessment shall also consider and include the following aspects:

[6] 'Problematic legislation' is understood as legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR

i. whether public authorities of the 3rd country may seek to access the personal data with or without the data importer's knowledge, in light of legislation, practice and reported precedents;

ii. whether public authorities of the 3rd country may be able to access the personal data through the data importer or through the telecommunication providers or communication channels in light of legislation, legal powers, technical, financial, and human resources at their disposal and of reported precedents;

iii. characteristics of the transfer (such as purposes, types of data, recipients, context, sector in which the transfer occurs, etc.);

iv. whether the data will be stored in the third country or whether there is remote access to data stored within the EU/EEA;

v. format of the data to be transferred (i.e. in plain text/ pseudonymised or encrypted);

vi. possibility that the data may be subject to onward transfers from the third country to another third country.

8.4 The assessment might also conclude that the initial risks related to the problematic legislation are in fact not relevant and such legislation or practice does not in fact pose any risks identified by monitoring. In that case, this Section 8 does not apply apart from the obligation to document and keep such assessment.

8.5 **Decision**. Following such assessment, Piano Group shall make a documented decision on such transfer. In situations (i) and (ii) above, Piano Group can either suspend the transfer or implement adequate supplementary measures that would allow it to proceed with such transfer. In situation (iii) above, in addition to options under previous sentence, Piano Group can alternatively decide to proceed with the transfer without implementing supplementary measures if it can be demonstrated and documented that there is no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice to cover the transferred data and the importer. If the decision is to continue on the basis of supplementary measure, these should be documented within the decision.

8.6 **Supplementary measures**. Supplementary measures are technical, legal, contractual or organizational measures that are adopted on top of measures and guarantees under these BCRs. The aim of these supplementary measures is to outweigh or balance the negative impact of problematic 3rd country legislation so that these BCRs can be still considered an effective safeguard for such transfer of personal datal even if the 3rd country's legislation or practice might be problematic from EU standards' perspective. When adopting supplementary measures, Piano Group will primarily look at non-exhaustive list of examples of supplementary measures in Annex 2 of the Board's Recommendations 01/2020 (as updated or replaced). It may be ultimately found that no supplementary measure can ensure an essentially equivalent level of protection for the specific transfer. In those cases where no supplementary measure is suitable, Piano Group must avoid, suspend or terminate the transfer.

8.7 **Procedural steps**. Following the decision to adopt of supplementary measures Piano Group shall consider any procedural ore regulatory steps under these BCRs or in general, including the obligation to report to the competent SA under Section 7.10 above.

8.8 **Re-evaluation**. Any decision or assessment made under this Section 8 shall be regularly re-evaluated, at least on an annual basis. This is supplemental to general monitoring obligation under Section 7.9 above. Should the re-evaluation of the initial assessment or previous decision reveal that the supplementary measures are no longer effective in that 3rd country, Piano Group shall promptly suspend any such transfer affected.

8.9 **Guidelines**. The process described in Section 8 shall be implemented in line with any applicable guidelines, recommendations or opinions of the Board and competent SAs on this matter.

9 FINAL PROVISIONS

9.1 Any updates of these BCRs must be approved by the Slovak SA. Updates to the BCRs or to the list of the BCR Members are possible without having to re-apply for an approval by the Slovak SA (or any other SA) providing that:

(a) DPO keeps a fully updated list of the BCR Members and keeps track of and record any updates to the rules and provides the necessary information to the data subjects or the Slovak SA upon request;

(b) no transfer is made to a new BCR Member pursuant to these BCRs until the new BCR Member is effectively bound by the BCRs and can deliver compliance;

(c) any changes to the BCRs or to the list of BCR members should be reported once a year to the relevant SAs, via the competent SA with a brief explanation of the reasons justifying the update in line with Section 2.3 above;

(d) where a modification would possibly affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character), it must be promptly communicated to the Slovak SA;

while such updates of BCRs take effect when updated BCRs are first published.

9.2 For avoidance of doubt, approval of the Slovak SA (or any other SA) under Section 8.1 above is also not required for:

(a) change of any internal data protection policy, agreement or document of Piano Group (DPAs, Group Policy, Privacy Policy, etc.);

(b) non-substantial changes to the Group Data Processing Agreement that do not affect any commitments or safeguards in these BCRs;[7]

(c) translation of these BCRs into other language versions;

(d) design, appearance, formatting or grammatical changes or updates of these BCRs;

(e) changes or updates to BCR annexes, provided that these do not affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character).

9.3 Any update of these BCRs must be without undue delay published at BCR Homepage and communicated to BCR Members and data subjects, where required under Art. 13 and 14 of the GDPR.

[7] These include mainly changes required by operational need to update of the purposes of processing, legal basis or updating of specification of the undertaken processing of personal data based on Group Data Processing Agreement. Any substantial changes or substantial deviations from the current wording of the Group Data Processing Agreement or any indirect changes to the wording, commitments or generally level of protection by these BCRs must be approved by the Slovak SA per Section 8.1.

ANNEX A: DEFINITIONS

These BCRs use terms in the same meaning as prescribed to them in Article 4 of the GDPR. In addition, for the purposes of these BCRs the following terms shall have the following meaning:

"**Agreement**" means "Piano Master Services Agreement Terms and Conditions" concluded between Piano and its Clients;

"**Applicable Data Protection Law**" means any local data protection or privacy legislation of the EU/EEA member state applicable to Piano Group;

"**BCR**" or "**BCRs**" means these binding corporate rules of Piano Group acting as a controller;

"**BCR Homepage**" means Piano Group's landing page (www.piano.io/bcr) dedicated to information about these BCRs where copy of these BCRs, BCR Members, Complaint Form and any other related information about BCRs can be easily accessed;

"**BCR Members**" mean Piano Group entities which acceded to these BCRs pursuant to these BCRs (individually as the "**BCR Member**");

"**Board**" means the European Data Protection Board (formerly Article 29 Working Group);

"**Clients**" means Piano clients (such as publishers) on behalf of which Piano processes personal data as their processor (individually as the "**Client**") (not subject to these BCRs);

"**Complaint Form**" means the complaint available to data subjects pursuant to the Section 6 of these BCRs substantially in the form as prescribed in Annex D;

"**Controller**" means Piano Software Group that acts as the legal person, which determines the purposes and means of the processing of personal data;

"**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**DPIA**" means the data protection impact assessment pursuant to the Article 35 of the GDPR;

"**DPE**" or "**DPEs**" means the appointed data protection executive(s);

"**DPO**" means the appointed group data protection officer of Piano Group;

"**DPO File**" means the internal storage or file of the DPO containing the most important data protection related documentation;

"**GDPR**" means regulation (EU) 2016/679 of the European parliament and 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 (General Data Protection Regulation);

"**Group Data Processing Agreement**" means the data processing agreement concluded by all Piano Group entities as per Annex C hereto;

"**Group Policy**" means the internal and non-public data protection policy of Piano Group which is not part of these BCRs;

"**EEA**" means European Economic Area encompassing the EU, Norway, Iceland and Lichtenstein;

"**EU**" means the European Union;

"**ISM**" means information security manager of Piano Group;

"**Personal Data**" means any information relating to Data Subject such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject;

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**Special categories of personal data**" mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited;

"**Piano**" or "**Piano Group**" means collectively Piano Software, Inc., Philadelphia, US and any and all its subsidiaries and affiliates;

"**Piano Slovakia**" means Piano Software, s.r.o., with seat at Štefánikova 14, Bratislava 811 05, Slovakia, company ID No. (IČO): 46 103 406;

"**Privacy Policy**" means the privacy policy of Piano Group in line with Art. 13 and 14 of the GDPR published on its website or elsewhere;

"**SA**" means the supervisory authority pursuant to the Article 4 (21) of the GDPR;

"**Slovak SA**" means the Office for Personal Data Protection of the Slovak Republic (www.dataprotection.gov.sk);

"**Services**" mean services provided by Piano to its Clients on the basis of the Agreement;

"**Software**" means Piano software provided by virtue of Services;

"**US**" means the United States of America.

ANNEX B: BCR MEMBERS

The following Piano Group entities are the first BCR Members. Signatories below hereby declare that they are duly and fully authorized to legally represent the BCR Member. By signing below, the BCR Member accedes to the Piano Group BCRs, agrees with its contents and accepts the obligation to comply with the these (controller) BCRs including with the Group Data Processing Agreement that forms inseparable part of these controller BCRs.

	BCR Member	Country[8]	Contact	Signatures
1.	**Piano Software, Inc.,** 111 S Independence Mall East, Suite 950, Philadelphia, PA 19106, United States, ID No.: 4151404	**United States (third country)**	Stuart Ashford stuart.ashford@piano.io	_____
2.	**Piano Software, s. r. o.**, Štefánikova 14, 811 05 Bratislava, Slovak Republic, Company ID No.: 46 103 406	Slovakia (EU)	Stuart Ashford stuart.ashford@piano.io	_____
3.	**Newzmate Sp. z o.o.**, ul. Mazowiecka 11 lokal 49, 00-052, Warsaw, Mazowieckie, Poland, ID No.: 360486660	Poland (EU)	Alex Chapko security@piano.io	_____
4.	**Piano Software B.V.**, Keizersgracht 555, 1017 Amsterdam, The Netherlands, ID No.: 75524171	The Netherlands (EU)	Alex Franta security@piano.io	_____
5.	**Piano Software Norway NUF**, Drammensveien 165, 0277, Norway, ID No. 923 967 850	Norway (EEA)	Alex Franta security@piano.io	_____
6.	**Piano Co. Ltd**, 2F Harajuku Jingu-no-mori Building, 1-14-34, Shibuya-ku, Tokyo, Japan, ID No. 1011001071838	**Japan (third country)**	Ryoichi Egawa security@piano.io	_____
7.	**OOO "Pi-Tech"**, Leninsky, 111, bldg. 1, floor 3, room 26, of. 40, 119421, Moscow, Russia, ID No. 7728493442	**Russia (third country)**	Kirill Kouterguine security@piano.io	_____
8.	**Piano Software Singapore PTE. Ltd.,** 16 Raffles quay #33-03 Hong Leong building Singapore (048581), ID No. 202031085R	**Singapore (third country)**	Tim Rowell security@piano.io	_____
9.	**Applied Technologies Internet SAS,**	France (EU)	Mathieu Llorens security@piano.io	_____

[8] Country refers to location where establishment of the BCR Member is located. One BCR Member might have more than one establishment. Although usually the establishment is where the registered seat of the company is located, the term establishment might also cover location of the corporate presence, office, store, branch or desk of a company other than its registered seat.

	85 avenue J F Kennedy 33700 Mérignac, France Trade and Companies Register of Bordeaux as number 403 261 258			
10.	**Applied Technologies Internet GmbH,** Leonrodstrasse 52-58, 80636 Munich, Germany Trade and Companies Register of Munich as number HRB 194384	Germany (EU)	Mathieu Llorens security@piano.io	_____
11.	**AT Internet holding SAS,** 4 Rue de Marivaux 75002 Paris, France Trade and Companies Register of Paris B 893 718 106	France (EU)	Trevor Kaufman security@piano.io	_____
12.	**AT Internet LTD,** 23 Copenhagen Street, London, N1 OJB, United Kingdom, ID No. 06740401	**UK (third country)**	Mathieu Llorens security@piano.io	_____

ANNEX C: GROUP DATA PROCESSING AGREEMENT

This **Group Data Processing Agreement** is concluded by and between **Piano Software Inc.**, located at 111 S Independence Mall East, Suite 950, Philadelphia, PA 19106, United States (for the purpose of this Group Data Processing Agreement as "**Piano**") and all other BCR Members ("**Affiliated Companies**"), collectively referred to herein as the "**Parties**" or the "**Group**" by virtue of adherence to the BCRs and by becoming BCR Member and in line with Article 26 of the GDPR.

WHEREAS:

(1) The Group represents a group of undertakings pursuant to the Article 4 (19) of the GDPR, where Piano acts as a controlling undertaking and the Affiliated Companies act as controlled undertakings;

(2) Parties have jointly determined their own (internal) purposes and means of processing their own personal data within the Group, while personal data are mutually shared, used or otherwise processed by different legal entities;

(3) Parties use joint internal systems for processing and exchange of their own data and for collaboration of their personnel;

(4) Parties wish to explicitly agree on the scope and distribution of the joint controllers' obligations stemming the Article 26 GDPR;

THEREFORE, PARTIES AGREED AS FOLLOWS:

1. **Definitions**. The terms used in this Group Data Processing Agreement shall be interpreted and construed in accordance with GDPR. As used in this Group Data Processing Agreement, the following terms shall have the following meanings:

   "**BCR**" or "**BCRs**" means Piano Group's approved binding corporate rules for the controller activities;"

   "**Group Staff**" means any employees, workers, directors or officers of the Group;

   "**Joint Contact Point**" means contact point of the Parties acting as joint controllers, in particular the following contact details: privacy@piano.io, postal: Piano Software, s.r.o., ATTN: Piano Group DPO, Štefánikova 14, 811 05 Bratislava, Slovak Republic;

   "**Piano Purposes**" or "**Purposes**" means purposes determined jointly by Parties acting as joint controllers as described in more detail in the Privacy Policy;

   "**Privacy and Data Protection Requirements**": the national applicable law "implementing" the GDPR, the Electronic Communications Data Protection Directive (2002/58/EC), the national applicable law implementing the e-Privacy Directive, GDPR, the European ePrivacy Regulation, as and if enacted, and all applicable laws and regulations relating to the processing of the personal data and privacy, including any other national data protection authority, and the equivalent of any of the foregoing in any relevant jurisdiction;

   "**Privacy Policy**" means the Group privacy policy published and regularly updated by the DPO at www.piano.io/privacy.

2. **Subject-matter**. Subject-matter of this Group Data Processing Agreement is the agreement of Parties on joint processing of personal data pursuant to the Article 26 of the GDPR and on defining their mutual responsibilities as regards Piano Purposes.

3. **Duration and Termination**. This Group Data Processing Agreement is concluded for an indefinite period of time. Parties acknowledge that is impossible to undertake business and effectively operate without processing personal data pursuant to this Group Data Processing Agreement. Therefore, this Group Data Processing Agreement can only be terminated or changed at the sole discretion of Piano. Affiliated Companies agree to accept any changes or amendments to this Group Data Processing Agreement proposed by Piano.

4. **Position of the Affiliated Companies**. Piano and Affiliated Companies act joint controllers for Piano Purposes. Parties agree with such an appointment and obligations stemming thereof.

5. **Purposes and Legal Bases**. The Group is processing personal data for the following Piano Purposes, while the Privacy Policy may describe these purposes and legal bases in more detail, without the need to change this intragroup data processing agreement:

Purposes of processing	Legal basis
1. Employment purposes	Legal obligation, performance of contract and legitimate interest
2. Employee monitoring	Legitimate interest
3. Intra-group sharing of personal data for administrative purposes	Legitimate interest
4. Tax and accounting purposes	Legal obligation
5. Establishment, exercise or defense of legal claims (legal agenda) (including AML)	Legitimate interest, legal obligation
6. Protection of assets and security (including fraud prevention)	Legitimate interest, legal obligation
7. Development, testing and updating of the software / products	Legitimate interest
8. Direct marketing and PR purposes	Legitimate interest, consent
9. Archiving purposes	Legal basis of the original purpose in line with Article 89 GDPR (recital 50 GDPR), legal obligation
10. Statistical purposes	Legal basis of the original purpose in line with Article 89 GDPR (recital 50 GDPR)

6. For avoidance of doubts, the above purposes of processing might need to be further specified towards data subjects in the privacy notices or information pursuant to the Article 13 or 14 GDPR. Each BCR Member is obliged to provide additional information under previous sentence, where necessary, in accordance with the Applicable Data Protection Laws. As regards other personal data, Affiliated Companies are allowed to process such data for its own purposes not falling under Piano Purposes only after notification to the Group DPO, while such processing is not subject to this Group Data Processing Agreement, unless the DPO instructs otherwise.

7. **Types of Personal Data**. The types of processed personal data typically include name, surname, date of birth, birth number, position, address, phone number, email, photo, data in the scope of CV and other typical types of HR / personnel data including any data related to usage of internal IT systems and infrastructure of the Group, typical business, legal and contract data related to performance of contract with business partners and typical marketing data including information collected via cookies or similar technologies (such as the specific content accessed, time and duration of the visit, IP address, geographical location of the end-user device, offer conversion and/or interaction data, referring site, user profile, information about data subject consent or objection or other information or other information relating to such natural person collected via

Group marketing tools, social media profiles or websites).

8. **Categories of Data Subjects**. Personal data processed by joint controllers will mostly relate to Group Staff, potential employees of any Group member, vendors, service providers and advisors of the Group and their employees, users of Group IT infrastructure, visitors of Group's websites, social media profiles, employees or representatives of Group's contractors or any third party whom the Piano Purposes might related to.

9. **Processors and Transfers**. As regards Purposes, Affiliated Companies shall: (i) not be entitled to appoint another sub-processor or a third party to process the personal data without Piano's prior consent; (ii) only use its Group Staff for processing of the personal data; (iii) comply with this Group Data Processing Agreement, applicable internal rules, procedures and policies and BCRs, if applicable. Parties agree that as regards Purposes, only Piano is authorized to conclude data processing or joint controllers' agreements with third parties also for the benefit of the whole Group. Affiliated Companies will adhere to section 7.20 (Processors and transfers) of BCRs and will notify to the DPO any intention to use processors or joint controllers regardless of whether BCRs apply in the given situation or not.

10. **Data Subject Rights**. As regards Purposes, Affiliated Companies are not entitled to handle or respond to the data subject requests. Should any Affiliated Company receive a data subject request that is of general nature and might be or is related to the Purposes, its shall immediately forward such request to DPO without undue delay. All data subject requests are handled and responded by the DPO. Parties agreed to use the Joint Contact Point for receiving any data subject requests regarding Purposes.

11. **Transparent Information**. Parties will use the Privacy Policy to encompass all information to data subjects pursuant to the Article 13 or 14 GDPR covering all Parties acting as joint controllers. Any other information to be provided to data subjects pursuant to the Article 13 or 14 GDPR by any Party must be first consulted with DPO. The Joint Contact Point shall always be part of the Privacy Policy or any information provided by Piano pursuant to Article 13 and 14 GDPR. In addition, pursuant to Article 26 (2) of GDPR, Parties agreed that the following essential parts of the joint controller's agreement contained herein will be published via the Privacy Policy:

"The essence of the joint controllers' agreement is following:

- ***Piano entities collaborate in joint processing activities related to all here mentioned own purposes of processing of Piano Group for which personal data may be shared and transferred vis-a-vis Piano entities;***
- ***We have established a single contact point for data subjects, as per this privacy policy;***
- ***Internally, all data subject request are handled by Piano Group DPO;***
- ***Our main establishment is located in Slovakia;***
- ***Our leading supervisory authority for data protection matters is the Office for Protection of Personal Data of the Slovak Republic (www.dataprotection.gov.sk);***
- ***Piano Software, Inc. is authorized to conclude data processing or joint controllers agreement for the benefit of the whole Piano Group."***

12. **Confidentiality**. Parties are obliged to comply with the internal policies among others in respect to (i) ensuring that access to the Personal Data by Group Staff is limited to what is necessary to

achieve the Purposes and (ii) ensuring that Group Staff are committed to the confidentiality in respect to the personal data.

13. **Internal Policies**. Affiliated Companies are obliged to comply with any the controller's instructions as well as with the Group Policy, rules, procedures or standards in respect to the security, protection of personal data, privacy as adopted by Piano. For clarity, Parties will comply with the following internal policies when processing the personal data in connection with this Group Data Processing Agreement:

13.1 BCRs. BCRs set out data protection safeguards as regards the Cross-Border Processing.

13.2 Group Data Protection Policy. Group Data Protection Policy set outs Group procedures for handling personal data mainly in respect to the data subject requests based on Piano Purposes, internal compliance measures in respect to the personal data generally, roles and responsibilities of key Group Staff and specific obligations of the Group stemming from the GDPR (the "**Group Data Protection Policy**") .

13.3 Information Security Policy. Information Security Policy set outs Group technical and physical safeguards for protection of confidential information including the personal data, roles and responsibilities of the key Group Staff, employee discipline and termination procedures and acceptable use policy (the "**Information Security Policy**").

13.4 Other Policies. Other policies might include password policy, incident response plan, disaster avoidance and recovery plan, system security plan, application and software development security (the "**Other Policies**").

BCRs, Group Data Protection Policy, Information Security Policy and the Other Policies are hereinafter referred to as the "**Internal Policies**".

14. **Security**. In addition to complying with the Internal Policies, Affiliated Companies are obliged to comply with any additional obligations stemming from the DPA, including those related to general client data obligations and obligation to adopt and comply with appropriate security measures.

15. **Assistance**. Affiliated Companies are obliged to assist Piano or if Piano requests so assist the Client with complying with any additional obligations stemming from the Privacy and Data Protection Regulations, mainly the GDPR. In any case Affiliated Companies are obliged to immediately notify Piano any potential or actual regulatory or court action or request in respect to the personal data processed in connection with this Group Data Processing Agreement.

16. **Audit**. As Affiliated Companies agree to be bound accept internal audit by Piano or its external advisors if deemed necessary by Piano for data protection or meeting Piano's obligations.

17. **Main Establishment**. Pursuant to the Article 4(16) of the GDPR, the main establishment of the Group is the place of its central administration in the EU and/or the establishment in the EU where the main processing activities take place to the extent that Group is subject to specific obligations under the GDPR. Parties acknowledge that the main establishment of the Group in respect of the Purposes is Slovakia. As a result, the Slovak SA will act as the lead supervisory authority of the Group pursuant to the Article 56 of the GDPR.

18. **BCRs**. Affiliated Companies / BCR Members agree to be bound by and comply with BCRs.

19. **3rd Party Beneficiaries**. Parties hereby explicitly agree to allow 3rd party beneficiaries to rely and bindingly enforce against any Party 3rd party beneficiary rights guaranteed under Section 4 of BCRs.

ANNEX D: COMPLAINT FORM

Compliant Form

under Piano Software Binding Corporate Rules

1. Practical information

About this complaint mechanism

This complaint form can be used by any individual / person that believes his or her personal data are processed by any Piano Software entity that acceded to the so-called Binding Corporate Rules (**BCRs**). The text of the BCRs and list of BCR Members is available at www.piano.io/bcr. BCRs require Piano Software to adopt a specific complaint handling mechanism as a means of additional safeguard for privacy and data protection principles. Data subjects are free to use this complaint form, but they are also free to draft the complaint and deliver it to Piano Software as they see fit. This complaint form is therefore not mandatory.

When to use complaint?

You can use the complaint whenever you like. For example:

- when you feel that Piano Software's BCR Members do not comply with text of the BCRs or applicable data protection laws when processing your personal data;
- if you would like to enforce any 3rd party beneficiary clauses against any BCR Member as per Section 4 above; or
- if you would like to enforce any data subject right pursuant to Articles 15 to 22 GDPR.

The more you explain the above in your complaint, more effectively will be your complaint dealt with by us. Therefore, in your complaint, please explain in detail why you are lodging the complaint, on what grounds and what specific rights are you enforcing, if any.

Where to complain?

You can fill out and submit this form in an online version available at www.piano.io/bcr which is the most effective and recommended option. You are also free to draft your own complaint at deliver it to Piano Software's group Data Protection Officer by email at dpo@piano.io or in writing by post to Piano Software, Group DPO, Piano Software, s.r.o., Štefánikova 14, 811 05 Bratislava, Slovak Republic.

How will your complaint be handled by us?

Your complaint will be handled internally by our group Data Protection Officer typically within 1-month period. In limited circumstances this period can be prolonged by another 2-months considering the complexity and overall number of the requests. In any case, you will receive a final response, prolongation notification or request for additional information within the original 1-month period, by email or post, depending on your selected preferences. Please note that when we receive data subject request in relation to operations we conduct as processors (on behalf of our clients), we are normally obliged to forward such request to our clients, and we do not respond directly.

Each complaint is dealt with individually by our privacy and data protection professionals in light of your specific circumstances. Complaints are handled by our group Data Protection Officer with relevant regional data protection officers and relevant data protection executives. We do not use software or automated tools to handle similar requests or complaints.

Before we provide a final response to your complaint, we might need to verify your identity or request additional information from you that is needed for handling the complaint. Until this additional information is provided to us, we cannot provide the final response. In this light, please provide as much detail to your compliant as necessary.

What are the consequences in case of rejection of compliant?

If we reject your complaint, this practically means we will not change the way how your personal data is handled or generally how we operated before the complaint. If we unduly rejected your complaint, you would still have legal options to enforce your compliant against us.

What are the consequences in case the complaint is considered as justified?

If we consider your complaint justified, we will adopt measures to comply with these BCRs or the Applicable Data Protection Law, as requested. We will also confirm in a response to you, what measures have been adopted to comply with your complaint.

What are the consequences if you are not satisfied by our reply?

If you are not satisfied with our reply or with how we handled your complaint (or generally at any time), you have right to:

- lodge a claim before any competent court;
- lodge a complaint before any competent supervisory authority.

The fact that Piano Software Group has its lead supervisory authority in Slovakia (Office for Personal Data Protection of the Slovak Republic, web: https://dataprotection.gov.sk/uoou/en) does not prevent data subjects to lodge complaints before other supervisory authorities.

As per Article 77 GDPR, every data subject has the right to lodge a complaint with a supervisory authority, in particular in:

- the Member State of his or her habitual residence;
- place of work or;
- place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

The list of competent supervisory authorities in the EU can be found at the website of EU Commission (https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm) as well as on the BCR Homepage (www.piano.io/bcr).

As per Article 79 GDPR, every data subject has the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed. Such court claim can be brought before the courts of the Member State where:

- Piano Software Group has an establishment (see the list of BCR Members); or where
- the data subject has his or her habitual residence.

What rights do you have under GDPR?

If you use this complaint mechanism to enforce your data subject rights under GDPR, we list below a basic overview of these rights. Please note, that most of these rights are not absolute and certain conditions must be met in most cases for such rights to apply. Two of the most automatic rights where no additional conditions need to be met are:

- **right to withdraw your consent** with processing personal data under Article 7 or 8 GDPR;

- **right to object against direct marketing** including the profiling under Article 21 (2) GDPR.

In both cases, we must automatically stop the relevant processing of your personal data based on such requests without further conditions. In addition, you have following rights under GDPR:

- **Right to access** to your personal data under Article 15 GDPR, including (i) confirmation as to whether we process your personal together with all relevant information under Article 15 (1) GDPR; (ii) right to be informed about transfers of personal data and appropriate safeguards under Article 15 (2) GDPR; and (iii) right to receive copy of personal data undergoing processing under Article 15 (3) GDPR;
- **Right to rectification** of incorrect personal data under Article 16 GDPR;
- **Right to erasure (right to be forgotten)** under Article 17 GDPR;
- **Right to restriction of processing** under Article 18 GDPR;
- **Notification obligation regarding rectification or erasure of personal data or restriction of processing** under Article 19 GDPR;
- **Right to portability of personal data** in a structured, commonly used and machine-readable format under Article 20 GDPR;
- **Right to object** against legitimate interests, public interest, direct marketing and profiling under Article 21 GDPR;
- **Right not to be subject to an automated individual decision making** under Article 22 GDPR**.**

In addition, you have right to be notified about certain data protection breaches under Article 37 GDPR and we shall seek your views within certain data protection impact assessments under Article 35 GDPR. However, these provisions are drafted as our direct obligation, not data subject rights.

2. Text of the complaint

Type of information needed:	**Please fill out here:**
Basic identification and contact data:	Name and surname: Residence: Email: Mobile phone:
What is your relationship to Piano Software Group or individual BCR Member?	*For example, are your our employee, contractor, business partner, recipient of marketing communication, etc.?*
Please identify whether this compliant is addressed to any specific BCR Member or BCR Members or generally against all BCR Members:	
Please specify what type of request or complaint are you lodging:	□ complaint on not complying with BCRs or applicable data protection laws by any BCR Member; □ enforcement of any 3-rd party beneficiary rights as per Section 4 BCRs;

	□ general data subject request as per Article 15 to 22 GDPR.
Please specify what rights (if any) are you enforcing with this request or complaint:	*In case of enforcement of any 3-rd party beneficiary rights as per Section 4 BCRs and general data subject request as per Article 15 to 22 GDPR.*
Please explain in more detail content of your request or complaint as per the above:	*For example what parts or provisions of BCRs or laws you think were infringed by us or what type of right under GDPR are you enforcing?*
How would like to receive response from us?	☐ by email ☐ by post

ANNEX E: TEMPLATE FOR PERSONAL DATA BREACH DOCUMENTATION

This record was drafted by the group DPO of the Piano Software, Inc. (the "Controller") acting in the capacity of joint controllers with other BCR Member in compliance with Article 33 (5) of the GDPR[9] and serves to document the breach and evidence of the security measures and procedures to mitigate the risk for the rights and freedoms of natural persons (hereinafter referred to as "Record").

Whereas:

(A) In light of Article 4 point 12 of the GDPR: "*personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"* (hereinafter referred to as "Breach").

(B) In light of Article 33 (5) of the GDPR: „*The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*"

The Controller has decided to document the Breach as follows:

1.	**Date, location, time of the finding of Breach and its internal signature:**	*/stating date, location and exact time of the finding of the Breach and it is also recommended to number the Breach internally/*
2.	**Contact information of the DPO:**	*/title, name, surname, email and phone number/*
3.	**Contact information of the Chief of Security:**	*/ title, name, surname, email and phone number /*
4.	**Contact information of other persons with significant knowledge of the Breach:**	*/e.g. internal employee who contacted the DPO regarding the Brach/*
5.	**Basic Description of the Breach:**	*/DPO states in his/her own words what actually happened/*
6.	**BCR Members affected by the breach:**	*/DPO states whether the Breach affects specific BCR Members, the whole group, or whether some BCR Members were not affected at all./*
7.	**How the Brach was found:**	*/e.g. missing documents or files, automatic notification from the security software, notifying unusual network activity phenomena, logging data analysis notification, employee report, reporting to an IT consultant, notification from a processor, DPO's activity, mediation, receiving suspicious e-mail, receiving a cyber request for a ransom attack, Ddos Attack Online Services Features, Knowledge Acquired as a result of Applying Employer Control Devices to Employees, etc./*
8.	**Description of the nature of the Breach:**	*/description of a specific event that has been identified and that has the potential to jeopardize or violate the integrity,*

[9] Article 35 (5) of the GDPR: *"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*

		confidentiality, or availability of information that contains personal data. The event that has led to the accidental or unlawful destruction, loss, alteration, unauthorized provision of personal data or unauthorized access to information containing personal data should also always accurately characterized. At the same time, the list of data subject concerned and their estimate and the number of threatened or compromised data (e.g. number of records and data size in MB, GB, TB) should be reported to the data subjects affected by the Breach and their (approximate) number./
9.	**Identification of the security measures taken to prevent the occurrence of the Breach:**	*/specification of the security measures and procedures that were intended to provide the protection against the emergence of an identified Breach within the internal policies, guidelines or security projects/*
10.	**Possible causes of the Breach:**	*/in the case of a Breach that results in high risk for the rights and freedoms of natural persons the internal investigation and audit of the Controller shall aim to identify the causes of the Breach, describing all relevant facts that have had an impact on the origin, impacts of the Breach detected/* */it is also recommended to provide a chronological description of the course of the incident, a description of the threats that have been made, the identification of the vulnerabilities that have been used and the way it has taken place, it is also advisable to list the affected assets affected by the breach, to identify and define the overriding security measures, if the breach has occurred despite the adoption of an adequate security measure and the foreseeable reason for overcoming such a security measure/* */it is also advisable to record what specific security measures or practices have been violated if there is a causal link between the occurrence of the Breach and the Breach and attempt to identify the person or persons responsible for the violation of the obligation and the internal rules in connection with the Breach/*
11.	**Relationship of the Breach and residual risk for the rights and freedoms of natural persons:**	*/the nature of the Breach in relation to residual risks and uncovered risks that the DPO has documented e.g. in security project under the previous legislation/*
12.	**Description of the likely consequences of the Breach:**	*/description of the identified and potential negative impacts of the Breach not only on the assets but also, the duty of confidentiality, the persons to whom the personal data in question were concerned, the legitimate interests of the client/*
13.	**Description of the measures taken or proposed to remedy the Breach:**	*/all actions that have been or are being proposed to be executed in specific terms by authorized personnel shall be listed to remedy the breach/*
14.	**Description of the measures intended to mitigate the adverse effects of the Breach:**	*/The DPO indicates all actions that have been or are being proposed to be executed with specific deadlines by authorized personnel to mitigate the adverse consequences of Breach/*

15.	**Proposed updates to security measures:**	*/ The DPO documents what steps have been taken to prevent similar incidents such as the Breach in the future./*
16.	**Assessment of the obligation to notify the data protection authority pursuant to Article 33 GDPR:**	*/ The DPO answers the question: Is the Breach likely to result in a risk for the rights and freedoms of individuals? Justification of the statement./*
17.	**Assessment of the obligation to notify the data protection authority pursuant to Article 34 GDPR:**	*/ The DPO answers the question: Is the Breach likely to result in a high risk for the rights and freedoms of individuals? Justification of the statement. /*
18.	**Date and time of notification to the data protection authority:**	*/ the exact date and time of the notification shall be stated and written evidence of the execution of notification shall be enclosed - to be completed only if the notification has been filed/*
19.	**Reasons for missing the deadline for notification of the Breach to the data protection authority:**	*/ reason for failure to comply with the time period of 72 hours (3 days) - to be filled in only if the deadline was missed /*
20.	**Date and time of notification to data subjects:**	*/ the exact date and time of the notification as well as the manner of notifying the Breach in relation to the data subject shall be stated./*
21.	**Statement by the Statutory Body of the Controller (optional):**	*/ the statutory body shall express its views on the Breach and approve the next procedure (in particular the decision on the notification / non-notification of the Breach /*

Based on the above documentation, the Controller has decided:

☐ To not notify personal data breach to the supervisory authority pursuant to the Article 33 of the GDPR; *„because the Breach is **unlikely to result in a risk** to the rights and freedoms of natural persons "*

☐ To not notify personal data breach to the supervisory authority pursuant to the Article 33 of the GDPR; *„ because the Breach **is likely to result in a risk** to the rights and freedoms of natural persons "*

☐ To notify personal data breach to the data subjects pursuant to the Article 34 GDPR *„ because the Breach **is likely to result in a high risk** to the rights and freedoms of natural persons "*

☐ To not notify personal data breach to the data subjects pursuant to the Article 34 GDPR *„ because the Breach **is unlikely to result in a high risk** to the rights and freedoms of natural persons "*