Data Protection Policy

1. This Policy defines requirements to ensure compliance with laws and regulations applicable to the ATPI's collection, use, Processing, and transfer of Personal Data throughout the world.

2. **Scope**

2.1 ATPI is committed to complying with the applicable Data Protection Laws in the countries in which it (the "**Company**") operates. Because of differences within these jurisdictions, the Company has adopted this Data Protection Policy which creates a common core of values, policies and procedures intended to achieve generic compliance, supplemented (where applicable) with additional instructions and guidance applicable in those jurisdictions with unique requirements.

2.2 This Policy is based upon EU Regulation 2016/679 and the General Data Protection Regulation (GDPR), which provides a robust generic model for privacy compliance. The Company has also established an Intra Group Data Transfer Agreement (IGDTA) based on the recognized EU Model Clauses, to be authorized for worldwide transfer, and subsequent sub-Processing, of Data throughout its entire global network of group companies.

2.3 This Policy applies to all Company full and part time employees, agency employees, and all suppliers and clients who receive Personal Data from the Company, have access to Personal Data collected or Processed by the Company, or who provide information to the Company, regardless of geographic location.

2.4 As a Policy commitment, the Company will not process Personal Data without a recognized legal basis for such processing. To ensure compliance with Data Protection Laws, the Company will correctly establish its status for all Data Processing as either a Data Controller, or Data Processor acting for another Data Controller.

3. **Group Compliance**

3.1 The Company's data compliance program will be overseen by the Head of Group Compliance (HGC) assisted by locally appointed compliance staff and internal auditors. Responsibilities may be delegated by the HGC.

3.2 The HGC will implement the Company's international Data Protection Policy and procedures and IGDTA, as well as any duties required by Data Protection Laws, including:

3.2.1 Determining whether notification to one or more Data Protection Authorities is required as a result of the Company's Data Processing activities, then making any required notifications, and keeping such notifications current.

3.2.2 Designing and implementing ongoing programs for training employees to ensure compliance with Data Protection Laws.

3.2.3 Establishing (with the involvement of the IT and legal departments) procedures and standard contractual provisions for obtaining compliance with this Policy by group companies, clients, suppliers, and third parties who receive Personal Data from the

Company, have access to Personal Data collected or processed by the Company, or who provide information to the Company, regardless of geographic location.

3.2.4 Establishing mechanisms for periodic audits of compliance with this Policy, implementing procedures, and applicable law.

3.2.5 Establishing, maintaining, and operating a system for prompt and appropriate responses to Data Subject requests to exercise their rights.

3.2.6 Establishing, maintaining, and operating a system for the prompt and appropriate automatic disclosure to the relevant authorities and Data Subjects of any loss of Personal Data.

3.2.7 Informing senior managers, officers, and directors of the Company of the potential corporate and personal civil and criminal penalties which may be assessed against the Company and/or its employees for violation of applicable Data Protection Laws.

3.2.8 Ensuring that the risk management plans in relation to Data Protection is implemented effectively and promptly.

3.2.9 Ensuring that adequate assurance regarding the effectiveness of Data Protection procedures and audits is provided to the Board, management and other stakeholders.

4. **Data Protection Principles**

4.1 The Company has adopted the following principles to govern its use, collection, Processing and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

4.1.1 Personal Data shall only be Processed fairly and lawfully.

4.1.2 Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further Processed in any manner incompatible with those purposes.

4.1.3 Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or Processed.

4.1.4 Personal Data shall not be collected or Processed unless a legal basis for Processing is properly established.

4.2 Appropriate physical, technical, and procedural measures shall be taken to:

4.2.1 Prevent and/or to identify unauthorized or unlawful collection, Processing, and transmittal of Personal Data; and

4.2.2 Prevent accidental loss or destruction of, or damage to, Personal Data.

5. **Transfers to Third Parties**

5.1 Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to establish and maintain the required level of Data Security.

5.2 Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the Data was originally collected or other purposes authorized by law.

5.3 All transfers of Personal Data to third parties for further Processing shall be Subject to written agreements, a legal basis for transfer, or under the Company's IGDTA for internal Data transfers.

5.4 EU Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless the transfer is made to a country or territory recognized by the EU as having an adequate level of Data Security or to the United States under the EU-US Privacy Shield, to which the Company is registered.

5.5 Subject to the provisions of the above, Personal Data may be transferred where any of the following apply:

5.5.1 The Data Subject has given Consent to the proposed transfer;

5.5.2 The transfer is necessary for the performance of a contract between the Data Subject (either personally or via his employing company as a client of the Company) and the Company;

5.5.3 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a third party or the employer of the Data Subject;

5.5.4 The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;

5.5.5 The transfer is required by law;

5.5.6 The transfer is necessary in order to protect the vital interests of the Data Subject.

6. **Prevention of Non-Complying IT Systems**

6.1 The Company's Chief Information Officer (CIO) shall establish a procedure for assessing the impact of any new or existing Technology on the privacy and security of Personal Data.

6.2 No new system or new version of an existing system shall be made available for use until the HGC has obtained written confirmation from the CIO that there would be no breach of any Data Protection Laws.

7. Sources of Personal Data

7.1 Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the Data from other persons or bodies.

7.2 If Personal Data is collected from someone other than the Data Subject, the business unit collecting the Data must have confirmation, in writing, from the supplier of the Data that there is a lawful basis for the Processing and the transfer of the Personal Data to the Company.

8. **Data Subject Rights**

8.1 Data Subjects shall be entitled to obtain the information about their own Personal Data held by the Company by making a written request in the format **here**, whereby the request will be recorded.

8.2 The Company shall provide its response to a request above within 40 days from the date of the written request, or within a shorter timescale if required by applicable Data Protection Laws.

8.3 Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data held about them.

9. **Sensitive (Special Category) Data**

9.1 Sensitive Personal Data should not be processed unless:

9.1.1 Such Processing is specifically authorized or required by law.

9.1.2 The Data Subject expressly and unambiguously Consents.

9.1.3 Where the Data Subject is physically or legally incapable of giving Consent, but the Processing is necessary to protect a vital interest of the Data Subject. This exemption may apply, for example, where emergency medical care is needed.

9.1.4 Data relating to criminal offenses may be processed only by or under the control of the Legal Department.

10. **Data Quality Assurance**

10.1 Personal Data must be kept only for the period necessary for permitted uses. The Company has established a Data Retention Policy which determines applicable timescales for Data deletion.

10.2 Personal Data shall be erased if its storage violates any Data Protection Law or if knowledge of the Data is no longer required by the Company, or at the request of the Data Subject.

11. Intra-Group Processing

11.1 Where the Company relies on another group company to assist in its Processing activities, the Company will enter into a Data Transfer Agreement based upon the EU Model Clauses with that other group company in order to ensure that responsibility for the data is clearly identified, as both parties may be considered as Data Controllers.

11.2 Where the other group company is located abroad, the group companies involved in the Processing shall be known as a Data Exporter and a Data Importer respectively, although there may be more than one Data Importer involved in the Processing.

12. Third Party Processors.

12.1 Similarly where the Company relies on third parties to assist in its Processing activities, the Company will choose a Data Processor who provides sufficient security measures and takes reasonable steps to ensure compliance with those measures, and in the case of any third party within the US, that they are also registered for the EU-US Privacy Shield.

13. **Written Contracts for Third Party Processors.**

13.1 The Company shall enter into a written contract with each Data Processor requiring it to comply with Data Protection Laws and security requirements imposed on the Company under local legislation.

14. **Audits of Third Party Data Processors.**

14.1 As part of the Company's internal Data auditing process, the Company shall conduct periodic checks on processing by third party Data Processors, and in particular relating to the hand-off procedures for the Data especially in respect of security measures.

15. **Notice to Directors, Managers, and Officers of Potential Sanctions for Non-Compliance**

15.1 The HGC shall notify directors, managers, and other officers of the Company that:

15.1.1 Failure to comply with relevant Data Protection Laws may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and

15.1.2 They can be personally liable where an offence is committed by the Company with their consent or connivance, or is attributable to any neglect on their part.

16. **Data Security**

16.1 The Company has implemented a Data Security Management Policy, under which it shall adopt physical, technical, and organizational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized Processing or access, having regard to the nature of the Data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. These measures will be documented within the Data Security Management Policy, which will be reviewed at least annually, or when necessary to reflect significant changes to security arrangements.

16.2 Adequate security measures should include all of the following:

16.2.1Prevention of unauthorized persons from gaining access to Data Processing systems in which Personal Data is processed.

16.2.2 Preventing persons entitled to use a Data Processing system from accessing Data beyond their needs and authorizations.

16.2.3 Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a Data carrier cannot be read, copied, modified or removed without authorization.

16.2.4 Ensuring that Personal Data is protected against undesired destruction or loss.

16.2.5 Ensuring that Data collected for different purposes can and will be processed separately.

16.2.6 Ensuring that Data is not kept longer than stipulated in the Data Retention Policy, including by requiring that Data transferred to third persons be returned or destroyed.

17. Compliance Measurement.

17.1 The HGC shall establish a schedule for and implement a privacy compliance audit for all business units. The HGC, in cooperation with the business units, shall devise a plan and schedule for correcting any identified deficiencies within a fixed, reasonable time.

17.2 Each Company business unit shall review annually its Data collection, Processing, and Data Security practices and shall determine what Personal Data the business unit is collecting including that held in manual systems that constitute "Relevant Filing Systems".

17.3 The information collected in this annual review shall be delivered to the HGC for review and appropriate action including, without limitation, the following:

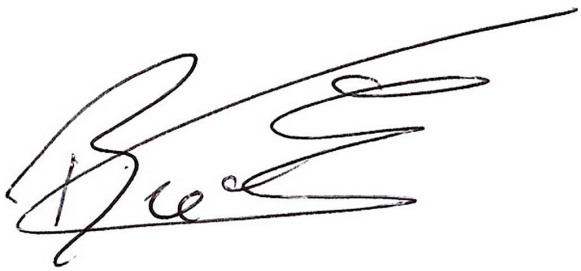
17.3.1 Making recommendations for improvement to policies and procedures in order to improve compliance with this Policy and applicable law.

17.3.2 Satisfying the requirements for self-certifying compliance within local Data Protection Authorities, and compliance with the Company's own IGDTA.

18. Implementation.

18.1 This Policy shall be available to employees through the Company compliance system, and an abridged public version shall be made available to others via the Company's website.

18.2 This Policy may be revised at any time but at least annually by the HGC. Notice of significant revisions shall be provided to employees through the company compliance system and to others via the Company's website.



January 2021

Michael Beacher
Head of Group Compliance

Appendix A

Glossary

Consent: Consent means "any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed."

Nevertheless, Consent may be obtained by a number of methods. These may include clauses in employment contracts, check boxes on replies to application or purchase forms, and click boxes on online forms where Personal Data is entered.

In most European Union countries, Consent to the Processing of Sensitive Personal Data needs to be clear and unequivocal. This generally means that some form of specific, active Consent) is required. This requirement is sometimes found to be less unequivocal beyond the EU.

Data: Data (whether or not having an initial capital letter) as used in this Policy shall mean information which either:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;
- does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital Data by computer or automated equipment, telephone recordings, and any manual information which is part of a Relevant Filing System.

Data Controller: Data Controller means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data is, or is to be, processed. Generally, Company itself will be the Data Controller in most cases.

Data Exporter: Data Exporter means the Data Controller or Data Processor who transfers the personal data abroad.

Data Importer: Data Importer shall means the Data Controller or Data Processor who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of this Policy and the relevant Data Transfer Agreement.

Data Processor: Data Processor means any person, other than an employee of the Data Controller, who processes the Data on behalf of the Data Controller. A company may be a Data Processor if defined as such under contractual terms with the Data Controller.

Data Protection Authority: A body that is tasked with the protection of data and privacy. The authorities are set up to uphold information rights in both the public and private interest.

Data Protection Laws: The Data Protection Act 2018 and the General Data Protection Regulation (regulation EU 2016/679); any data protection legislation outside of the EU within countries in which ATPI operates; and Electronic Communications (EC Directive) Regulations 2003 and any revisions thereof.

Data Security: Measures that the Controller and Processor must implement for compliance with the data protection principles by design and default and to ensure a level of security appropriate to the risk to the rights and freedoms of individuals, taking account of the state of the art, the cost of implementation and the nature, scope, context and purposes of processing.

Data Subject: Data Subject means the person to which Data refers. Data Subjects include customers and web users, individuals on contact /e-mailing lists or marketing Databases, employees, contractors and suppliers.

EU-US Privacy Shield: A framework constructed by the US Department of Commerce and the European Commission to enable transatlantic data protection exchanges for commercial purposes. The EU-US privacy shield enables companies from the EU and the US to comply with data protection requirements when transferring personal data from the EU to the US.

Personal Data: Personal Data means Data related to a living individual who can be identified from those Data or from those Data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor. Personal data does not include information that has been anonymized, encoded or otherwise stripped of its identifiers, or information that is publicly available, unless combined with other non-public personal information.

Processing: Processing covers a wide variety of operations relating to Data, including obtaining, recording or holding the Data or carrying out any operation or set of operations on the Data, including:

- Organisation, adaptation, or alteration;
- Disclosure by transmission, dissemination, or otherwise; and
- Alignment, combination, blocking, erasure, or destruction.

'Processed' shall be construed accordingly.

Relevant Filing System: Relevant Filing System means any set of information relating to individuals, whether kept in manual or electronic files, structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Therefore any digital Database and/or organized manual files relating to identifiable living individuals fall within the scope of Data Protection laws and regulations, while a Database of pure statistical or financial information (which cannot either directly or indirectly be related to any identifiable living individuals) will not.

Sensitive Data: Sensitive Data means Personal Data containing information as to the Data Subject's:

- Race or ethnic origin;
- Religious beliefs or other beliefs of a similar nature;
- Political opinions;
- Physical or mental health or condition;
- Sexual history or orientation;

- Trade union membership;
- Commission or alleged commission of any offense and any related court proceedings.

Technology: Technology is to be interpreted broadly, to include any means of collecting or Processing Data, including, without limitations, computers and networks, telecommunications systems, video and audio recording devices, biometric devices, closed circuit television, etc.

Link to DSA request form
Link to GDPR Privacy Notice