BASS DATA PRIVACY COMPLIANCE POLICY

Document Name: BASS Data Privacy Compliance Policy	Date: 1st April 2023
Approved By: Per Steinar Upsaker / CEO – Managing Director	Version No: 01
Document Owner: Doris Henrietta John – Data Protection Officer	

Table of Contents

BASS Data Privacy Compliance Policy

Introduction

The ***EU General Data Protection Regulation ("GDPR")*** comes into force across the European Union on 25th May 2018 and applicable Data Privacy Laws in other regions globally, it brings with it the most significant changes to data protection law in the last two decades. Based on privacy by design and taking a risk-based approach, the GDPR and Data Privacy Laws has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across primarily across the EU and its sub-processors across the globe; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

BASS is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always taken precautionary actions to ensure we adhere to the existing laws and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the relevant Data Privacy Laws in other regions is significant.

BASS is dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR / Data Privacy compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

GDPR/Data Privacy Compliance Procedure

The company have conducted privacy impact assessments of our current processors to review and improve risk areas whilst providing additional features in new product versions to become and remain compliant to GDPR / Data Privacy Laws.

BASS already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR/ Data Privacy Law requirements as processors. *Our preparation includes: -*

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- ***Policies & Procedures* – Review and implement restricted access to comply with** data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data privacy laws, including: -
    - ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR / Data Privacy. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

    - ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
    - ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time.
    - ***International Data Transfers & Third-Party Disclosures*** – where BASS stores or transfers personal information outside the EU, we have procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information.
- ***Privacy Notice/Policy*** – we have revised our Privacy Notice(s) to comply with the GDPR/Data Privacy, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** - we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials. Our website provides avenues for our visitors to provide their contact information for requests such as product demo or enquiry. By providing us with the information, we will contact them to fulfill their request.

- ***Indirect Marketing*** – BASS uses cookies to provide a seamless and meaningful online experience to users that visits our website. The cookies are small files sent to devices to understand user behavior and display contents relevant to lifestyle. Users can be assured that BASS have developed preventive measures to further avoid the use of persistent cookies in regards to non-retention of login details, passwords associated with personal data with options to accept or decline cookies compliant with GDPR requirements.
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR / Data Privacy obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data*** - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via Human Resource System and documented into BASS Data Privacy Policy of an individual's right to access any personal information that BASS processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this

- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws

Information Security & Technical and Organisational Measures

BASS takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have secured security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -**Access controls, (password policy, encryptions, pseudonymisation, practices, restriction and IT, authentication etc]**

GDPR / Privacy Roles and Employees

BASS have appointed **Data Protection Officer (DPO)** to develop and implement our roadmap for complying with the new data protection Regulation. The DPO is responsible for promoting awareness of the GDPR / Data Privacy Laws across the organization, assessing our GDPR / Data Privacy readiness, identifying any gap areas and implementing the new policies, procedures and measures.

BASS understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR / Data Privacy and have involved our employees in our preparation plans. GDPR / Data Privacy Training programs forms part of our induction and annual training program.

Please contact the undersigned, if you have any questions.

Doris Henrietta John
Doris.henrietta@bassnet.no
Data Protection Officer