Group Data Protection Policy

Version: 3.0
Published: 24/03/2023

Doc Reference: DP-GCC-01.01

Version Control & Sign Off

Version	Sign off obtained by:	Sign off date:
1.0	William Hill General Counsel	28/01/2021
2.0	Chief Risk & Compliance Officer, William Hill	23/03/2022
3.0	Executive Risk & Sustainability Committee	17/03/2023
	Board of Directors	24/03/2023

Related Documents

- Executive Risk & Sustainability Committee Terms of Reference
- Divisional data protection policies
- Information security policies

1. Purpose

1.1. The purpose of this policy is to set out the framework for data protection compliance within 888 Holdings PLC.

1.2. This policy outlines the function of the Data Protection Officer, data protection compliance department, and responsibilities of people included within the scope of this policy.

2. Scope

2.1. 888 Holdings PLC including all group companies, staff, and affiliates ("888" / "Group" / "Staff").

2.2. Where requirements of this policy are applicable to any person or entity within the Group, it shall also be applicable to any third-party or contractor where appropriate.

3. Policy

3.1. The Group shall comply with data protection and data privacy regulations as they apply to the Group's operations within the Group's risk appetite.

3.2. The Group employs a Data Protection Officer ("DPO") who is supported by the data protection compliance department to ensure compliance with data protection regulations in accordance with the Group's risk appetite.

3.3. The DPO and data protection compliance department sits within the Risk and Compliance function in Group Corporate Centre and provides data protection compliance services to the entire Group.

3.4. Responsibilities of the DPO:

3.4.1. The DPO shall have the statutory responsibilities as outlined in data protection regulations such as the General Data Protection Regulation ("GDPR") or any other equivalent regulation containing similar requirements that is applicable to 888's business.

3.4.1.1. The DPO can delegate aspects of their role to members of data protection compliance department, other staff, or contractors to execute the statutory requirements of the DPO at their discretion.

3.4.2. The DPO is responsible for managing the Group's data protection compliance framework to ensure the Group is compliant with data protection regulations in accordance with its risk appetite.

3.4.3. The DPO has the authority to establish committees and working groups to support data protection compliance, approve policy and process relating to data protection compliance, and negotiate data protection compliance points with external parties in the Company's interest.

3.4.4. The DPO is a point of escalation for data protection compliance related matters including suspected or confirmed personal data breaches.

3.4.5. The DPO will escalate data protection compliance risks to the Executive Risk and Sustainability Committee and the Chief Risk Officer as appropriate.

3.4.6. Where the Group experiences a data protection compliance issue that could require a regulatory notification, the DPO is responsible for determining whether such incident is reportable to the regulator. Where the issue is a reportable incident the DPO is responsible for ensuring a timely notification is made to relevant regulators.

3.4.7. The DPO is responsible for the effective management of the data protection compliance department.

3.4.8. The DPO shall be the Key Function Holder or equivalent role holder for any data protection or privacy related betting and gaming licence requirements.

3.5. The DPO leads the data protection compliance department. This department supports the DPO in ensuring the Group is compliant with data protection regulations within risk appetite. Specifically, the data protection compliance department is responsible for:

3.5.1. Advising on data protection compliance matters in a timely manner, recommending measures to achieve compliance and mitigating any compliance risk with minimal commercial impact, as far as is possible.

3.5.2. Designing and implementing processes to ensure the Group is compliant with data protection requirements in accordance with risk appetite.

3.5.3. Assist the DPO in managing data protection compliance risks and alerting the Chief Risk Officer or the Executive Risk and Sustainability Committee (as appropriate) to data protection related risk they become aware of and to provide advice on how the Group can reduce or eliminate the risk.

3.5.4. Actively engaging with departments that support data protection compliance such as Legal and Information Security.

3.5.5. Facilitating data protection compliance training.

3.5.6. Ensuring that data rights requests are responded to compliantly.

3.5.7. Maintaining a log of personal data breaches that are reported to the data protection compliance team.

3.5.8. Owning the Group's relationship with all data protection and privacy regulators including responding to their enquiries and engaging in consultations.

3.5.9. Ensuring business units are supplied with sufficient management information satisfy reporting requirements.

3.6. Responsibilities of Staff:

3.6.1. Engaging and consulting with the data protection compliance department in a timely manner on any matters that can impact the Group's compliance with data protection and data privacy regulations.

3.6.2. Reporting and escalating data protection compliance issues to the data protection compliance department.

3.6.3. Following the advice and instructions of the DPO and the data protection compliance department and implement appropriate technical and organisational measures to achieve compliance with data privacy and data protection laws. Any decision to ignore the advice given, must be specified in writing, outlining the circumstances and reasons for this.

3.6.4. Reporting personal data breaches or breaches of data protection compliance in accordance with relevant incident management processes.

3.6.5. Complying with any additional policies and procedures relating to data privacy, data protection compliance and information security.

3.6.6. Completing mandatory training in data protection compliance and any supplementary training provided by the data protection compliance department.

3.6.7. Work with the data protection compliance department to ensure third-party suppliers are compliant with data privacy and data protection regulations.

3.6.8. Keep personal data secure at all times and comply with the Group's information security policies.