GDPR Policy for Pulse Communications Ltd

1. Introduction

Pulse Communications Ltd ("the Company") is committed to ensuring the security and protection of the personal data that I process and to providing a compliant and consistent approach to data protection. This policy outlines my compliance with the General Data Protection Regulation (GDPR) and my responsibilities regarding the collection, use, storage, and protection of personal data.

---

2. Scope of the Policy

This policy applies to all employees, contractors, and stakeholders of Pulse Communications Ltd and governs all personal data processed by or on behalf of the Company. This includes data related to clients, employees, suppliers, and any other identifiable individual.

---

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Processing**: Any operation performed on personal data, whether automated or not.
- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes data on behalf of the Data Controller.

---

4. Principles of Data Protection

Pulse Communications Ltd adheres to the principles of data protection as outlined in the GDPR. Personal data shall be:

1. **Lawfully, fairly, and transparently processed**: I ensure transparency in how data is collected and used.
2. **Collected for specific, explicit, and legitimate purposes**: Data is processed only for the purposes stated at the time of collection.
3. **Adequate, relevant, and limited**: Data collection is limited to what is necessary for the intended purposes.

4. **Accurate and up to date**: Data inaccuracies are rectified without delay.
5. **Stored no longer than necessary**: Retention periods are established for each type of data.
6. **Securely processed**: Appropriate security measures are in place to protect data.

---

5. Rights of Data Subjects

Data subjects have the following rights under GDPR:

- **Right to Access**: Individuals can request access to their personal data.
- **Right to Rectification**: Individuals can request corrections to inaccurate or incomplete data.
- **Right to Erasure**: Individuals can request the deletion of their data.
- **Right to Restrict Processing**: Individuals can limit how their data is used.
- **Right to Data Portability**: Individuals can obtain and reuse their data across different services.
- **Right to Object**: Individuals can object to specific types of processing.
- **Right not to be subject to automated decision-making**: Individuals are protected from decisions made solely by automated means.

Requests related to these rights can be made via email to **[insert contact email]**. I will respond within one month, as required by GDPR.

---

6. Legal Basis for Processing

Pulse Communications Ltd processes personal data based on one or more of the following legal grounds:

- **Consent**: Explicit consent has been obtained from the data subject.
- **Contractual Obligation**: Processing is necessary for the performance of a contract.
- **Legal Obligation**: Processing is required to comply with the law.
- **Legitimate Interests**: Processing is necessary for the legitimate interests of the Company, provided these do not override the data subject's rights.

---

7. Data Security

I implement and maintain appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data. These measures include:

- Encryption and secure storage systems.
- Regular security assessments and audits.
- Access controls to limit data access to authorised personnel only.

---

8. Data Retention

Pulse Communications Ltd retains personal data only for as long as necessary to fulfil the purposes for which it was collected. Once the retention period expires, data is securely deleted or anonymised.

---

9. Third-Party Processors

I ensure that any third-party processors engaged by Pulse Communications Ltd are GDPR-compliant and adhere to my data protection standards. Contracts with third parties include specific data protection clauses to safeguard personal data.

---

10. Data Breaches

In the event of a data breach, the Company will:

1. Notify the relevant supervisory authority within 72 hours, if required.
2. Inform affected individuals if the breach is likely to result in a high risk to their rights and freedoms.
3. Document the breach, including its causes, effects, and remedial actions taken.

---

11. Training and Awareness

All employees and contractors are provided with training on GDPR compliance and data protection best practices. Regular updates and refreshers ensure ongoing awareness of responsibilities.

---

12. Policy Review

This policy is reviewed annually or whenever there are changes to relevant legislation or the Company's operations. Updates are communicated to all relevant stakeholders.

Effective Date: 17 November 2024