Arrow Group Data Breach Policy & Procedures

1. Policy Statement

The Arrow Group, including Arrow Business Communications Limited and Arrow Business Communications (Scotland) Limited (hereinafter referred to as the "Group") are committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance adherence and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any data breaches, this policy states our intent and objectives for dealing with such a breach.

Although we understand that not all risks can be completed mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from the risks associated with processing data. The protection and security of the data that we hold and use, including personal information, is paramount to us and we have developed data specific controls and protocols for any breaches involving personal information and data that is subject to the GDPR and data protection laws.

2. Purpose

The purpose of this policy is to provide the Group's intent, objectives and procedures regarding data breaches involving personal information. As a regulated company, we have developed this dedicated data breach policy that is specific to personal information and the breach requirements set out in the GDPR.

As we have obligations under the GDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees if a personal information breach occurs. This policy also notes our processes for reporting, communicating and investigating any such breach.

Whilst it is the Group's aim to prevent data breaches where possible, we do recognise that human error and risk elements occur in business that prevent the total elimination of any breach occurrence. We also have a duty to develop protocols for data breaches to ensure that employees, the supervising authority and regulating and/or accreditation bodies are aware of how we handle any such breach.

3. Scope

This policy applies to all staff within the Group (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Group in the UK or overseas), and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. Data Security & Breach Requirements

The Groups's definition of a personal data breach for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy be Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policy & Procedures and Data Protection Policy & Procedures provide the detailed measures and controls that we take to protect personal information and to ensure its continued security.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on a data subject(s). We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*): -

- Pseudonymisation and encryption of personal data
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluating the effectiveness of all measures and compliance with the data protection regulations and codes of conduct
- Frequent and rolling training programs for all staff in the GDPR, its principles and applying those regulations to each role, duty and the company as a whole
- Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
- Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Data Protection Officer

5. Objectives

- To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and staff – including their data, information and identity

- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of the data breach (*where applicable*) with immediate effect and at the latest, within 72 hours after having become aware of the breach

6. Data Breach Procedures & Guidelines

The Group has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Due to the nature of our business, the Group processes and stores personal information and confidential data and as such, we have developed a structured and documented breach incident program to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

We carry out frequent risk assessments, reviews, audits and gap analysis reports on all processing activities and personal data storage, transfers and destruction mechanisms, to ensure that our compliance processes, functions and procedures are fit for purpose and adequately mitigate the risks where possible.

7. Breach Monitoring & Reporting

The Group has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

8. Breach Incident Procedures

8.1 Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the reporting officer immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents fully and with immediate effect is essential to the compliant functioning of the Group and is not about apportioning blame. These procedures are for the protection of the Group, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

8.2 Breach Recording

The Group utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder *(electronic)* and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, the outcome of which is communicated to all staff involved in the breach, in addition to upper management. A copy of the completed incident form is filed for audit and record purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 6 of this policy*). The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form***' should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

9. Breach Risk Assessment

9.1 Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Group's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with the Group's disciplinary procedures)

9.2 System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

9.3 Assessment of Risk and Investigation

The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

10. Breach Notifications

The Group understands that we have obligations and a duty to report data breaches in certain instances. All staff are aware of these circumstances and we have strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without undue delay.

10.1 Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after us becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested.

Where the Group acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without undue delay after becoming aware of a personal data breach.

10.2 Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

11. Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

12. Responsibilities

The Group will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.