Policy for Dealing with a UK Data Subject Access Request (DSAR)

1. Introduction

This policy outlines the procedure for handling Data Subject Access Requests (DSARs) in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It ensures that requests are processed efficiently while maintaining data security and verifying the legitimacy of the requester.

2. Scope

This policy applies to all employees, contractors, and third parties involved in processing DSARs. It covers all requests for access to personal data held by the company.

3. Definitions

- **Data Subject:** An individual whose personal data is being processed.
- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Data Subject Access Request (DSAR):** A request by an individual to access their personal data.
- **Data Controller:** The entity that determines the purposes and means of processing personal data.

4. Legal Framework

Under the UK GDPR and DPA 2018, individuals have the right to access their personal data. This policy ensures compliance with these regulations, providing transparency and accountability in how DSARs are handled.

5. Principles

1. **Transparency:** Provide clear information on how to make a DSAR.
2. **Verification:** Ensure the identity of the requester before disclosing any personal data.
3. **Security:** Protect personal data from unauthorized access during the DSAR process.
4. **Timeliness:** Respond to DSARs within the statutory time frame.
5. **Compliance:** Adhere to legal requirements and best practices in data protection.

6. Procedure for Handling DSARs

6.1 Receiving a DSAR

1. **Request Channels:** DSARs can be received via email, post, or through a dedicated online form.
2. **Acknowledgement:** Acknowledge receipt of the DSAR within 5 working days.
3. **Record Keeping:** Log the DSAR in the DSAR register, including the date of receipt, requester details, and nature of the request.

6.2 Verification of Identity

1. **Initial Verification:** Request the following documents to verify identity:
    - A copy of a government-issued ID (passport, driver's license, etc.).
    - Proof of address (utility bill, bank statement, etc.).

2. **Additional Verification:** If there are doubts about the requester's identity, request further evidence such as:
    - Additional forms of ID.
    - Confirmation of specific data points only the data subject would know.

6.3 Assessing the Request

1. **Scope of Data:** Determine the scope of the requested data, ensuring it pertains to the requester.
2. **Clarification:** If the request is ambiguous or too broad, contact the requester for clarification.
3. **Legitimacy Check:** Ensure the request is legitimate and not part of fraudulent activities.

6.4 Gathering Data

1. **Data Collection:** Locate and gather the personal data related to the requester from all relevant sources.
2. **Data Review:** Review the data to ensure it does not infringe on the rights and freedoms of others.
3. **Third-Party Data:** Redact any information relating to third parties, unless explicit consent is provided or it is reasonable to disclose.

6.5 Response to the Request

1. **Time Frame:** Respond to the DSAR within one month from the date of receipt. If the request is complex, inform the requester that the period may be extended by a further two months.
2. **Format:** Provide the information in a structured, commonly used, and machine-readable format.
3. **Content of Response:**
    - A copy of the personal data.
    - Details on the purposes of processing.
    - Information on data recipients.
    - Retention periods for data.
    - Information on the data subject's rights.

7. Refusal to Comply with a DSAR

1. **Grounds for Refusal:** Refusal can occur if:
    - The identity of the requester cannot be verified.
    - The request is manifestly unfounded or excessive.
    - It infringes on the rights of others.
2. **Notification of Refusal:** Inform the requester of the refusal, providing reasons and information on their right to complain to the supervisory authority.

8. Data Security

1. **Access Controls:** Ensure that only authorized personnel handle DSARs.
2. **Data Transmission:** Use secure methods to transmit personal data to the requester.
3. **Data Storage:** Store DSAR-related data securely, with restricted access.

9. Training and Awareness

1. **Employee Training:** Provide regular training to employees on how to handle DSARs and data protection principles.
2. **Awareness Campaigns:** Conduct awareness campaigns to ensure all staff are informed about the importance of data protection and the DSAR process.

10. Monitoring and Review

1. **Regular Audits:** Conduct regular audits of DSAR handling processes to ensure compliance and identify areas for improvement.
2. **Policy Review:** Review this policy annually or in response to changes in legislation or business practices.

11. Complaints and Escalations

1. **Complaints Procedure:** Inform data subjects of the procedure to lodge a complaint if they are dissatisfied with the handling of their DSAR.
2. **Supervisory Authority:** Provide contact details for the Information Commissioner's Office (ICO) for unresolved complaints.

12. Conclusion

The company is committed to protecting personal data and ensuring that DSARs are handled in compliance with the UK GDPR and DPA 2018. This policy provides a clear framework for responding to DSARs, ensuring transparency, security, and accountability.