APPORTO'S DSAR (Data Subject Access Rights)

Effective Date: September 4, 2025

www.apporto.com

1. Introduction

Apporto Corporation complies with the General Data Protection Regulation (GDPR) by enabling data subjects to exercise their rights regarding personal data, as outlined in this Data Subject Rights policy document. This policy applies to all individuals whose personal data is processed by Apporto Corporation.

2. Data Subject Rights Under GDPR

Data subjects have the right to:

- Access their personal data
- Rectify inaccurate or incomplete data
- Erase personal data ("Right to be Forgotten")
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

3. How to Submit a DSAR

As a virtual desktop service, Apporto does not process or store individual user data. Individuals using one of Apporto's services should contact their organization to request their data be reviewed, corrected or deleted. If individual profiles (login usernames) or login logs need to be deleted, users should contact their Customer Admin within their organization. The Customer Admin would process their request internally and if needed, should contact Apporto with a Support Request Ticket for additional assistance.

4. Response Timeline

Apporto will respond to DSARs from the organization's Customer Admin within 30 calendar days of receipt. This may be extended by an additional 60 days for complex requests, with notification to the requester. Personal data will be provided in a structured, commonly used, and machine-readable

format (e.g., CSV or PDF). All DSARs and related correspondence will be documented and retained for compliance and audit purposes.

5. Information Provided

When notifying the customer of a vulnerability, Apporto will include comprehensive information that meets the disclosure requirements of UK GDPR, EU GDPR, and US state breach notification laws. The information provided will include the most detailed requirements from any applicable regulation.

6. Confidentiality

Apporto treats vulnerability information with strict confidentiality and expects the same from our customers. For certain high-severity vulnerabilities, Apporto may request that customers maintain confidentiality until a fix has been deployed to all affected customers.

7. Responsible Disclosure

Apporto practices responsible disclosure and will not publicly disclose vulnerabilities until:

- A fix or mitigation has been developed and tested
- The fix has been applied to all affected systems, or
- Affected customers have been notified and given reasonable time to implement mitigations

8. Continuous Improvement

Following any significant security incident, Apporto conducts a thorough post-mortem review to identify lessons learned and improve our security processes. Apporto may share anonymized findings with customers to help strengthen the security posture of our entire user base.

9. Regular Security Assessments

Apporto conducts regular security assessments, including:

- Vulnerability scanning
- Penetration testing
- Code reviews
- Third-party security audits

A summary of these assessments can be provided to customers upon request, subject to appropriate confidentiality agreements.

10. Legal and Regulatory Compliance

This policy has been developed to meet the most restrictive requirements across multiple jurisdictions and regulatory frameworks to ensure comprehensive compliance:

10.1 UK Regulations

- **UK GDPR and Data Protection Act 2018**: Personal data breach notifications within 72 hours to the Customer Admin, and without undue delay to affected data subjects when high risk is identified
- **NIS Regulations 2018**: Notification of significant cybersecurity incidents to relevant authorities within 24 hours for essential service providers
- **NCSC guidance**: Following National Cyber Security Centre best practices for vulnerability disclosure and incident management

10.2 EU GDPR Requirements

- **Article 33**: Notification to supervisory authorities within 72 hours of becoming aware of a personal data breach
- **Article 34**: Communication to data subjects without undue delay when breach is likely to result in high risk to rights and freedoms
- **Article 32**: Implementation of appropriate technical and organizational measures to ensure security of processing

10.3 US Regulatory Framework

- **State Data Breach Notification Laws**: Compliance with the most restrictive state requirements, including California's SB-1386 and other state laws requiring notification without unreasonable delay
- **NIST Cybersecurity Framework**: Adherence to NIST guidelines for incident response and vulnerability management
- **Sector-specific requirements**: Including HIPAA (where applicable), SOX, and other relevant federal regulations

11. Apporto's Unified Approach

To ensure compliance across all jurisdictions, Apporto applies the most restrictive standard from the above frameworks:

- **Personal Data Breach Notification**: Apportowill notify relevant authorities within **24 hours** (the most restrictive of UK NIS, EU GDPR 72-hour, and varying US state requirements)
- **Customer/Data Subject Notification**: Affected individuals will be notified **without undue delay and within 72 hours maximum** for high-risk breaches
- **Documentation**: All incidents will be documented in accordance with the highest standard required by any applicable regulation
- **Risk Assessment**: Apporto conducts comprehensive risk assessments using the most stringent criteria from all applicable frameworks

12. Escalation

If a data subject believes their rights have been violated, they may contact their local supervisory authority. A list of authorities is available here.

13. Contact Information

For questions about this policy or to report security concerns, please contact:

Apporto Security Team
Email: security@apporto.com

Document Review / Revision History

Date	Version	Action / Change	Reviewed / Approved By:
09.03.2025	1.1	Approved for release	Daniel Hutchison
09.02.2025	1.1	Policy creation	Nahum Nicholas

Effective Date: 09.03.2025
Review Cadence: At least annually
Other triggering events set out herein
Next Scheduled Review: 09.03..202