DFS GROUP

dfs sofology THE SOFA DELIVERY CO

Data Protection Policy

Document Owner:
Melissa Tasker

Version:
1.0

Contents

Document Control Summary

Version Control

V	Last Modified By	Change Description	Last Modified On
1.0	*Melissa Tasker*	*Document created*	*May 2026*

Review History

V	Document Owner	Review Comments	Reviewed Date
1.0	*Melissa Tasker*	*To be reviewed annually*	

Authorised by

V	Approver Name	Approver Role	Approved Date
1.0	*Julia Costello* *GRC*	*Group Head of Risk, Internal Controls and Compliance* *Governance and Risk Committee*	30 June 2026

Authorised by

V	Approver Name	Approver Role	Approved Date
1.0	*Group Board*	*Board of Directors*	9 July 2026

Related Documents

Document Name	Document Location
Data Protection Impact Assessment Data Protection: The Essentials	DPIA Template Data Protection: The Essentials

1. Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable living individual (e.g., name, email address, physical address, payroll number, online identifiers).
- **Data Protection Law**: Legal Framework that regulates how organisations, businesses, and government bodies collect, use, store, and share personal information. It is governed by a combination of complementary laws- UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data Use and Access Act (DUAA) and PECR (Privacy and Electronic Communications Regulations).
- **Special Category Personal Data**: Sensitive personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic/biometric data, health records, or data concerning an individual's sex life or sexual orientation.
- **Data Controller:** The entity that determines the purposes and means of processing personal data. For the purposes of this policy, DFS Furniture PLC and its subsidiary companies act as Data Controllers.
- **Data Processor**: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
- **Personal Data Breach**:a personal data breach is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. It extends well beyond simple physical loss or theft and impacts data confidentiality, integrity, or availability. Breaches can arise from human error (such as sending data to the wrong recipient) as well as intentional malicious activity (such as phishing or cyberattacks).

2. Introduction

2.1 This Data Protection Policy sets out how DFS Furniture PLC and subsidiary companies ("the Group", "we", "us", "our") handles the Personal Data of our customers, prospective customers, suppliers, employees, workers, business contacts, and other third parties. The Group is committed to protecting individual rights and handling personal data lawfully, responsibly, and transparently.

2.2 All processing of personal data is carried out in accordance with Data Protection Law. This policy establishes the principles, responsibilities, and governance arrangements through which the organisation ensures compliance and demonstrates accountability.

2.3 This policy applies to all employees of the Group ("you", "your"), and compliance is mandatory. Data protection is a shared responsibility across the organisation, and this policy sets out the explicit standards required to ensure the Group complies with applicable law.

2.4 When processing Personal Data on our behalf, you must:

(a) Read, understand, and comply with this Data Protection Policy.

(b) Complete all mandatory data protection training.

(c) Adhere to all related Group Policies and Privacy Guidelines.

3. Scope of Policy and When to Seek Feedback

3.1 This policy applies to all personal data processed by the Group, regardless of the format in which it is held, and to all individuals working on behalf of the organisation, including employees, contractors, and temporary employees. It covers both operational activities and any processing undertaken for research or innovation.

3.2 Please contact the Principal Data Steward or Compliance Team with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Principal Data Steward or Compliance Team in the following circumstances:

(a) Immediately, if there has been a Personal Data Breach (paragraph 8);

(b) if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Group) (see paragraph 5.2);

(c) if you need to rely on Consent or need to capture Explicit Consent;

(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 7);

(e) if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 6);

(f) if you want to transfer Personal Data outside the UK (see paragraph 9);

(g) if you need any assistance dealing with any rights invoked by a Data Subject or complaints (see paragraph 10)

(h) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 6) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 6);

(i) if you plan to undertake any activities involving Profiling or automated decision making(see paragraph 12);

(j) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 13); or

(k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 14).

4. Data Protection Principles

4.1 Personal data is processed in accordance with the core principles set out in Article 5 of the UK GDPR.

- Processed lawfully, fairly, and in a transparent manner (Lawfulness, Fairness, and Transparency).
- Collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner (Purpose Limitation).
- Adequate, relevant, and limited to what is necessary for the purposes for which they

are processed (Data Minimisation).

- Accurate and, where necessary, kept up to date (Accuracy).
- Kept in a form which permits identification of data subjects for no longer than is necessary (Storage Limitation).
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Integrity and Confidentiality).

5. Implementation of Principles

5.1 Lawfulness, Fairness, and Transparency
Personal data is processed only where a valid lawful basis exists under UK GDPR. This may include consent, contractual necessity, compliance with legal obligations, legitimate interests, or the performance of tasks carried out in the public interest or under official authority, as further clarified by the DUAA. Where special category data is processed, an additional condition is identified and recorded.

5.2 Individuals are informed, in clear and accessible language, about how their personal data is used and is available on the respective brands website. Privacy information is kept under review and updated where processing activities change.

- **Consent:** Explicit, clear, permission given by the data subject.
- **Contract**: Necessary to fulfill or enter into a commercial or employment contract.
- **Legal Obligation**: Necessary to comply with statutory legal mandates (e.g., HMRC tax accounting, employment laws).
- **Vital Interests**: Necessary to protect an individual's life.
- **Public Task:** Necessary for tasks performed in the public interest.
- **Legitimate Interests**: Necessary for corporate commercial operations, balanced strictly against the individual's underlying rights and expectations.
- **Special Category Standard:** Processing sensitive data requires a secondary legal justification under Article 9 of the UK GDPR, which must be fully documented and approved by the Compliance Team before processing starts.

5.3 Transparency and Customer Information
DFS provides detailed privacy notices to individuals at the point of data collection (e.g., via brand websites during checkout or account creation). These notices must be clear, written in plain language, and routinely updated to mirror any structural or system changes in data usage.

5.4 Purpose Limitation & Data Minimisation
Group Personnel must ensure that data collection is restricted to operational needs. For example, marketing sign-up webforms must not mandate physical addresses if a digital email address completely satisfies the interaction. Data collected for one purpose must never be repurposed without a formal compatibility assessment and an authorised lawful basis.

5.5 Data Accuracy
All business areas must take reasonable steps to ensure personal data is kept accurate and

updated. Inaccurate or obsolete records must be corrected or deleted without delay.

In line with ICO "Data Fundamentals," we adhere to the following:

(a) Minimalism: We proactively limit data collection to only what is strictly required for the business objective.

(b) Justification: Every designated retention period must be explicitly tied to a verified legal obligation or a legitimate business interest.

(c) Routine Review: Data sets across all business units are formally reviewed annually to systematically identify records ready for disposal or anonymization.

(d) Anonymisation: Where data is required for long-term trend analysis (such as evaluating seasonal sales volumes), it must be fully and irreversibly anonymized so that individual data subjects are no longer identifiable.

6. Data Protection By Design and Default

6.1 The DFS Group embeds data protection and privacy into the design, development, operation, and management of all business processes, systems, products, and services that involve personal data, in accordance with Article 25 of the UK GDPR. This framework applies universally to the processing of personal data relating to customers, employees, suppliers, visitors, and any other individuals who provide personal data to the organisation, regardless of the media or format in which that data is held.

6.2 The primary objective of these design principles is to guarantee that personal data is consistently:

- Processed lawfully, fairly, and transparently.
- Adequate, relevant, and limited strictly to what is necessary for its stated purpose.
- Protected securely throughout its entire lifecycle.

6.3 To ensure data protection is integrated into organisational workflows, the following principles must be adhered to across all business units:

- **Proactive Integration:** Data protection requirements must be evaluated from the earliest conceptual stages of any new or significantly modified product, service, system, business process, or technology deployment. Compliance must never be treated as an afterthought or rely solely on reactive controls.
- **Risk-Based Approach:** A proportionate, risk-based approach will be applied to all initiatives. This takes into evaluation the nature, scope, context, and purposes of the processing, alongside the volume, sensitivity, and likelihood/severity of risks to individual data subjects.
- **Data Minimization:** Systems and workflows must be intentionally designed to collect only the personal data that is strictly necessary, deliberately avoiding excessive or duplicated data collection. For example, marketing sign-ups must not mandate a full postal address if an email address alone is sufficient to fulfill the purpose.
- **Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes. Data must not be repurposed without a formal assessment and a valid lawful basis; any proposed secondary usage must be rigorously reviewed for compatibility with the original collection criteria.

6.4 A formal Data Protection Impact Assessment (DPIA) must be initiated and completed *before* commencing any processing operations that involve high-risk activities. A DPIA is strictly mandatory whenever the organisation introduces:

(a) New or unfamiliar technologies.

(b) Customer profiling or automated decision-making frameworks.

(c) CCTV, biometric authentication, or behavioral analytics systems.

(d) Large-scale or systematic monitoring of public or private spaces.

6.5 Operational step-by-step guidance on executing these assessments is detailed in the standalone **DPIA Policy and Framework**. All completed DPIAs must be formally reviewed and approved by the designated privacy lead before the project goes live.

6.6 Appropriate technical and organisational security controls must be engineered into all technical environments and applications from inception. Mandatory foundational baselines include:

- **Access Control:** Enforcing robust role-based access controls (RBAC) and secure authentication mechanisms for all employee-facing systems.
- **Data Safeguards:** Applying encryption protocols to personal data both at rest and in transit.
- **Oversight:** Maintaining detailed audit logging and active system monitoring to detect unauthorized actions.
- **Lifecycle End:** Building automated or secure manual data disposal and deletion mechanisms to enforce retention schedules.

7. Data Retention and Disposal

7.1 The Group has clear standards for retaining, managing, and securely disposing of all personal and business data throughout its lifecycle. By maintaining strict retention schedules and secure disposal methods, the organisation ensures that personal data is kept only for as long as necessary to fulfill its operational, legal, and regulatory obligations. This framework enforces robust data governance and ensures ongoing compliance with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

7.2 In relation to data retention principles and to ensure alignment with the Information Commissioner's Office (ICO) "Data Fundamentals" guidance, the organisation strictly adheres to the following core protocols outlined in paragraph 5.

7.3 Data must only be retained for the minimum period necessary to fulfill its original purpose, or to meet statutory limitation periods for legal claims. If a business unit intends to process existing data for a new or additional purpose, they must consult this policy or the *DPIA Framework* before proceeding.

7.4 The following operational retention periods represent the organisation's mandatory baselines which are managed and held by the appropriate functions:

Data Category	Retention Period	Rationale / Regulatory Basis
Recruitment Records	6–12 months	Defending potential discrimination claims.
Employment Contracts	6–7 years after the end of employment*	Limitation Act 1980 (breach of contract claims).
Payroll & Tax Records	6 years + current accounting year	HMRC audit requirements.
Health & Safety / Accident Records	3 years from the date of the incident**	RIDDOR compliance and injury claims.
Exposure to Hazardous Substances	40 years	Long latency period of occupational illnesses.
Pension Records	6 years after benefits cease	Resolution of long-term benefit disputes.
Retail Sales Contract Book	12 months	HMRC audit requirements.
Retail Cash Receipt Books	6 months	HMRC audit requirements.
Retail Cash Received Reports	6 months	HMRC audit requirements.
Supplier & Customer Delivery Notes	18 months	HMRC audit requirements.
Merchant Copies & Payment Receipts	4 weeks	HMRC audit requirements.

* Note: Employment contract data may be retained longer if there is an active, ongoing employment dispute .

** Note: Accident records may be retained longer if there is an active, ongoing personal injury claim.

7.5 Security and Safeguards During Storage
Personal and confidential data must be actively protected while it remains within its retention period:

- **Access Control:** Access to personnel files and sensitive records is strictly limited to authorised employees who require it specifically for their roles.
- **Electronic Security:** Mandatory encryption protocols and secure online portals must be used for sensitive data, including payroll and employee health information.
- **Physical Security:** Paper records must be stored securely in locked cabinets when not in active use. The creation of informal notes or "shadow" files outside approved systems is strictly prohibited.
- **Policy Compliance:** Full compliance with established IT security policies is required at all times; failure to adhere to these storage standards may result in disciplinary action.

7.6 Secure Disposal & Destruction Protocols
Once a retention period expires or data is flagged for deletion during an annual review, it must be completely destroyed using approved, non-recoverable methods:

- **Physical Records:** Paper documents must be shredded or disposed of using the designated confidential shredding bins provided at each Group site.
- **Digital Records:** Files must be permanently deleted, which requires emptying local "Recycle Bins" and ensuring data is purged from server backup cycles within the standard timeline (typically 30 days).
- **Hardware Lifecycle:** Decommissioned hard drives, storage media, or Point of Sale (POS) terminals must be physically destroyed or wiped using industry-standard sanitization software. The IT Department holds sole responsibility for verifying and executing the secure destruction of all IT equipment.

7.8 Legal Holds ("Stop the Clock" Protocol)
If the Group is formally notified of a legal dispute, an insurance claim, or a Data Subject Access Request (DSAR), the standard disposal and deletion of all relevant records must be suspended immediately.

7.9 Intentionally destroying, altering, or concealing records known to be relevant to an active investigation, legal dispute, or an open DSAR is a criminal offense under Section 173 of the Data Protection Act 2018. Data must not be deleted or altered until the legal hold is formally lifted by Risk and Compliance.

8. Data Breaches Response Framework

8.1 The DFS Group is committed to protecting the privacy, security, and statutory rights of individuals. This framework establishes the mandatory corporate approach to preventing, identifying, assessing, and managing personal data breaches in strict compliance with the UK GDPR, the Data Protection Act 2018, and official Information Commissioner's Office (ICO) guidelines.

8.2 The UK GDPR requires us to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject. We have put in place a framework to deal with any

suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

8.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. When a suspected or confirmed data breach occurs, the organisation must instantly activate the four-stage response framework.

8.4 Stage 1: Containment and Recovery

(a) **Immediate Escalation:** All employees must report any suspected or confirmed data breach immediately to the Compliance Team or Principle Data Steward. You should preserve all evidence relating to the potential Personal Data Breach and ensure confirmation of receipt is explicitly obtained.

(b) **Containment:** Where possible, the affected business unit must take immediate, proactive steps to isolate the issue and prevent further data loss.

(c) **Recovery:** Employees must immediately determine if data can be securely recovered or contained (e.g., executing an immediate email recall).

8.5 Stage 2: Risk Assessment

(a) The Compliance Team, with the direct assistance of the business area involved in the incident, will lead a formal investigation to determine if the breach is likely to result in a risk to the rights and freedoms of natural persons. The risk assessment evaluates:

(b) **Data Sensitivity:** Assessing whether "Special Category" data (such as health or biometric data) or criminal offense data is compromised.

(c) **Data Volume:** Verifying the total volume of records and the number of individual data subjects affected.

(d) **Existing Security Measures:** Determining if the data was encrypted, pseudonymized, or otherwise rendered unreadable to unauthorized parties.

(e) **Severity of Consequences:** Evaluating the potential real-world impact on individuals, such as identity fraud, financial loss, discrimination, or physical harm.

8.6 Stage 3: Notification Procedures

(a) **Regulatory Notification (To the ICO):** The Compliance Team assesses every incident on a case-by-case basis. Where an assessment indicates a breach is likely to result in a risk to individuals, a mandatory notification will be made to the ICO without undue delay and, where feasible, within **72 hours** of awareness. If a reporting decision is ambiguous, the ICO breach reporting tool will be used to validate the final path. Any notification submitted after the 72-hour window must include a justified reason for the delay.

(b) **Data Subject Notification:** If a breach is determined to present a *high risk* to individual rights and freedoms, the responsible business area must take immediate action. The Compliance Team will instruct the business area when this is necessary and provide hands-on drafting support.

(c) **Communication Standards:** All communications to affected data subjects must use clear, plain language and must contain a description of the breach, Compliance Team contact details, the likely consequences, and the active measures taken to mitigate the effects.

(d) **Data Processor Obligations:** Any contracted third-party data processor handling data on behalf of the organization is contractually and legally required to notify the organization of any data breach without undue delay upon becoming aware of it.

8.7 Stage 4: Post-Incident Evaluation

(a) **Cause Analysis:** Following containment, a formal post-incident review must be conducted to pinpoint the root cause of the breach.

(b) **Action Plan:** Technical controls, corporate policies, or employee training modules must be updated as necessary to eliminate the vulnerability and prevent recurrence.

(c) **Documentation:** Every single breach incident, regardless of whether it meets the statutory reporting threshold to the ICO, will be permanently recorded in an internal Breach Log maintained by the Compliance Team.

9. Transfer Limitation

9.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

9.2 You must comply with the Group's guidelines on cross-border data transfers.

9.3 You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Principle Steward;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including:

(e) the performance of a contract between us and the Data Subject;

(i) reasons of public interest;
(ii) to establish, exercise or defend legal claims;
(iii) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
(iv) in some limited cases, for our legitimate interest.

10. Data Subject's Rights and Requests

10.1 The DFS Group recognises and upholds the rights afforded to individuals under UK GDPR to control their own data. These include the rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the the Group's Processing activities;

(c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) request human intervention, make representations or challenge decisions based on Automated Decision Making (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and

(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

10.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

10.3 You must immediately forward any Data Subject request or complaint you receive to the Compliance team and comply with the Group's Response procedures for data subject requests. Please see related documentation.

10.4 If an individual is dissatisfied with the Group's handling of their personal data, they have the right to lodge a complaint with the Information Commissioner's Office (ICO). Individuals are encouraged to raise any concerns with the Group in the first instance, to allow an opportunity for the issue to be addressed promptly and effectively; however, this does not affect their right to escalate the matter directly to the ICO at any time. Further information on how to contact the ICO is available via their website.

11. Record Keeping

11.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

11.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with this policy.

11.3 These records should include, at a minimum:

(a) the name and contact details of the Controller; and

(b) clear descriptions of:

(i) the Personal Data types;

(ii) the Data Subject types;
(iii) the Processing activities;
(iv) the Processing purposes;
(v) the third-party recipients of the Personal Data;
(vi) the Personal Data storage locations;
(vii) the Personal Data transfers;
(viii) the Personal Data's retention period; and
(ix) the security measures in place.

11.4 To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

12. Profiling and Automated Decision Making (ADM)

12.1 Where we carry out ADM, we must have safeguards in place to:

(a) provide the Data Subject with information about the decision made about them;

(b) enable the Data Subject to make representations and to challenge the decision; and

(c) enable the Data Subject to obtain human intervention in relation to the decision.

12.2 If Special Categories of Personal Data are being processed for ADM, then we must not carry out such ADM unless a relevant condition as set out in the UK GDPR or Data Protection Act 2018 is met (for example, Explicit Consent).

12.3 When ADM is used, the Data Subject must be informed when we first communicate with them of the existence of this ADM, meaningful information about the logic involved and the significance and envisaged consequences for the Data Subject.

12.4 The Data Subject must also be able to make representations about these decisions (or express their point of view), obtain human intervention and contest or challenge the decision.

12.5 Where individuals are involved in any data Processing activity that involves Profiling or ADM, they must comply with the Group's guidelines on Profiling or ADM.

13. Direct Marketing

13.1 We are subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers. For example when sending marketing emails or making telephone sales calls.

13.2 For example, in a business to consumer context, a Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows an organisation to send marketing texts or emails without consent if it:

(a) Has obtained contact details in the course of a sale to that person.

(b) Is marketing similar products or services.

(c) Gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

13.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

13.4 A Data Subject's objection to direct marketing must always be promptly honoured. If a customer opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.5 You must comply with the Group's guidelines on direct marketing to customers and you should consult the Principal Data Steward if you are unsure regarding how to comply with either the Group's guidelines or the law.

14. Sharing Personal Data

14.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

14.2 You must comply with the Group's guidelines on sharing data with third parties.

14.3 You may only share the Personal Data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

14.4 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-compliant third party clauses has been obtained.

15. Accountability

15.1 The Group must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

15.2 The Group must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training employees on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Group must maintain a record of training attendance by Group Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Training and Audit

16.1 We are required to ensure all employees have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

16.2 All employees must undergo all mandatory data privacy-related training.

16.3 We must regularly review all the systems and processes under our control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

17. Compliance

17.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

17.2 We will terminate our relationship with any individual or organisation working on our behalf if they breach this policy.

18. Contacts

Group Compliance Mailbox	Email: Compliance@dfs.co.uk
Head of Risk, Internal Controls and Compliance	**Julia Costello** Email: Julia.Costello@dfs.co.uk Tel: **07894 400117**
Regulatory Compliance Manager	**Melissa Tasker** Email**:** Melissa.Tasker@dfs.co.uk Tel**: 07729095597**
Principal Data Steward	**Ronnie Bagdonavicius** Email: Ronnie.Bagdonavicius@dfs.co.uk Tel: **07706 345756**
Chief Legal & Business Assurance Officer	**Liz McDonald** Email: liz.mcdonald@dfs.co.uk Tel: **07849 083971**