DATA PROTECTION POLICY

POLICY NO. 04

VERSION: 1.0 **DATE OF LAST REVISION: 21.11.24** **OWNER: GROUP OPERATIONS**

VERSION HISTORY:			
VERSION	**APPROVED BY**	**REVISION DATE**	**KEY CHANGE**

SUMMARY

MUST DO

✓ All staff must comply with applicable data protection regulations.

- This policy outlines what RtD employees must to do to ensure compliance with data protection laws.
- The policy's objective is to ensure RtD employees understand their legal obligations with regards to what Personal Information may be legally obtained and retained.
- The policy outlines what personal data may be obtained and in what circumstances.
- The policy outlines how Personal Information must be stored and transmitted safely.
- The policy outlines how to process Data Subject Access Requests (DSAR sometimes known as SAR).
- The policy outlines retention periods for Personal Information.
- Audit and control processes are outlined.

TABLE OF CONTENTS

SECTION 1: SCOPE AND PURPOSE

Safeguarding personal and sensitive data is vital to maintaining trust and integrity within our organization. This policy ensures that all Right to Dream (RtD) employees, partners, and stakeholders understand their roles and responsibilities in protecting Personal Information.

SCOPE

This policy applies to all data collected, processed, stored, and transmitted by RtD, including but not limited to:

- Personal Information: Information relating to an identified or identifiable individual, such as names, addresses, email addresses, phone numbers, and social security numbers.
- Sensitive Personal Data: Special categories of personal data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, and data concerning a person's sex life or sexual orientation.
- Organizational Data: Proprietary information, intellectual property, and any data that is essential for business operations and strategic planning.
- Customer and Client Data: Any data entrusted to us by our customers and clients as part of our business relationships and service agreements.

This policy encompasses all Personal Information, regardless of the format in which it is held—digital, paper-based, or any other form—and covers all processes involving data handling, including collection, storage, processing, sharing, and destruction.

PURPOSE

The purpose of this Data Protection Policy is to:

- Ensure compliance: Adhere to all applicable data protection laws and regulations.
- Protect rights and freedoms: Safeguard the privacy and data protection rights of individuals whose data we process, ensuring their data is handled with the utmost care and respect.
- Mitigate risks: Identify and mitigate risks associated with data breaches, unauthorized access, data loss, and other security incidents.
- Promote transparency: Establish clear guidelines and procedures for data processing activities, ensuring transparency with data subjects about how their data is used and protected.

- Foster trust: Demonstrate our commitment to data protection and security to build and maintain trust with customers, clients, employees, and other stakeholders.

By implementing and adhering to policy, RtD aims to uphold the highest data protection standards, ensuring that all data handling practices are ethical, lawful, and aligned with our core values and strategic objectives.

SECTION 2: DEFINITIONS

- **Company** – Means Right to Dream Limited and subsidiary companies covering RtD Group, Denmark (FC Nordsjaelland A/S), RtD Ghana, RtD Egypt, and RtD US. It does not cover or apply to employees of San Diego, but does apply to any other future clubs and academies.

- **Employee** – Means all employees in the Company. Section 9 of the policy addresses the data protection rights of the Employees.

- **IT-systems and IT-equipment** - Means any form of hardware, software or portable devices which are utilized by the Company, including desktops, laptops, printers, cell phones, iPads and other "mobile devices", routers, WIFI etc.

- **Personal Information** - Means any information which are related to an identified or identifiable natural person (including names, mails, IP-addresses, license plates etc.)

- **Processing/Processed** - Means storage, transmission, systemization, communication, or other utilization of personal information in the Company's IT-systems, IT-equipment, or physical documents.

SECTION 3: RESPONSIBILITIES

ROLE	RESPONSIBILITIES
All RtD employees	• Must provide a written acknowledgement, verifying that they have been provided with the policy and have read and understood the contents of the policy. • Are required to comply with the guidelines and content of this policy.
People	• Inform new employees of the policy within 30 days of the employee being employed with the Company. • Ensures that all RtD employees are adequately trained and informed on the standard operating procedures governing their day-to-day work.
The Company	• Performs annual awareness and information training, focusing on data protection and handling of Personal Information. • Acts as a data controller for any Personal Information that concerns customers, partners, employees, suppliers or other individuals related to the Company.
The Head of Operations	• Ensures the Company's compliance with applicable data protection law, including the training of employees, awareness campaigns and internal controls intended to verify compliance. • Updates this policy annually or when relevant changes occur requiring an update.

POLICY OWNER

The Data Protection policy is owned by the Head of Operations, with the Group Head of Finance (hereafter Head of Finance) responsible for its implementation.

Local Finance Managers are responsible for ensuring local compliance and being a point of contact for Approvers when there are questions. They are also responsible for identifying opportunities to develop and implement the data protection procedures and processes locally.

SECTION 4: WHEN DOES RTD PROCESS PERSONAL INFORMATION

REGULAR PERSONAL INFORMATION

The Company shall only process Personal Information if one of the following conditions are met:

- processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- processing is necessary for the purposes of the **legitimate interests** pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

SPECIAL CATEGORIES OF PERSONAL INFORMATION

The Company shall only process Personal Information of one of the following conditions are met:

- the data subject has given explicit consent to the processing of those Personal Information for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Company or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by law or a collective agreement pursuant to law;
- processing relates to personal data which are manifestly made public by the data subject; or
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

SECTION 5: REVIEW AND UPDATING OF PROCEDURES

MUST DO

✓ Ensure all written procedures involving the processing of Personal Information are reviewed annually.

All written procedures involving the processing of Personal Information shall be reviewed annually.

The review shall focus on updating and/or verifying:

- the types of Personal Information are unchanged;
- the purpose of processing;
- that only necessary processing is performed;
- if the purpose can be achieved by processing less Personal Information;
- the legal basis for processing (see section 4);
- retention of Personal Information;
- the role of the Company as data controller or data processor;
- the duty to inform data subjects on of their rights; and
- if any data is transmitted outside EU.

SECTION 6: RIGHTS OF INDIVIDUALS

MUST DO	NEVER DO
✓ Answer any requests from data subjects within 14 days.	✘ Transmit any Personal Information without ensuring a proper legal basis is in place.
✓ Ensure any processed personal Information is correct.	

The Company has implemented procedures aimed at ensuring that data subjects are informed of their rights in accordance with applicable law. This information is generally provided, inter alia, in the bottom of all the Company e-mails, in the Company's terms and conditions, by sending an individual privacy notice to all relevant stakeholders.

The company people manager shall handle all data subject requests relating to the exercise of rights.

When assisting data subjects pursuant to 2 above, the Company shall verify that no Personal Information which does not relate to the data subject is delivered, deleted or affected by the request. Accordingly, the Company must verify the identity of any data subject requesting to exercise its rights.

The Company shall seek to answer any requests from data subjects within 14 days. All requests shall be fully expedited within 30 days. If a request is denied, the Company shall include a written statement explaining the reasoning.

The Company ensures that Personal Information processed is correct, by asking data subjects to verify that the Personal Information is correct and informing the data subject to reach out to the Company if the Personal Information be subject to change. Further, Personal Information which is relied upon for business transactions is periodically verified against public registries.

SECTION 7: ELECTRONIC PROCESSING AND SENDING OF PERSONAL DATA

MUST DO	NEVER DO
✓ Have a data processing agreement in place	✗ Transmit any Personal Information without ensuring a proper legal basis is in place.

USE OF DATA PROCESSORS

Before transferring Personal Information to a data processor, the Company must have a data processing agreement in place.

The relevant department manager is responsible for all data protection agreements within their department, assisted by the Company People manager.

A total registry of data processors and processing agreements shall be available in ComplianceLog, the Company's compliance management system.

The Company shall audit data processors annually. If the data processor processes large amounts or special categories of Personal Information, the Company shall enact extra security and audit measures that are in line with the risk-based approach.

TRANSMISSION OF PERSONAL DATA

Before transmitting Personal Information to entities outside the Company, the employee shall ensure that a proper legal basis is in place (see Section 4). If no legal basis can be established, the transmission shall be cancelled.

If Personal Information is transmitted to a third-party, the employee together with the relevant department manager and the Company People manager shall assess if the third-party shall be required to sign a confidentiality statement.

SECTION 8: RETENTION OF PERSONAL INFORMATION

MUST DO

- ✓ Verify that stored Personal Information is still required for the purpose it was collected.
- ✓ Monitor data retention periods through Compliancelog.

All employees shall verify on an ongoing basis if the Company's IT-systems or IT-equipment contains Personal Information which is no longer needed for the purpose which it was collected. If the employee concludes that Personal Information is stored without a valid purpose (or if the purpose has been exhausted), the Personal Information shall be deleted or anonymized. This also applies to Personal Information processed by a data processer.

Retention periods shall be monitored through Compliancelog, compliance management system. Each retention period set out below, shall be subject to appropriate controls (e.g., by way of spot-checking or similar) in the system verifying and documenting that retention periods are complied with.

RETENTION PERIODS

CUSTOMERS

Personal Information relating to customers is kept for 3 years after the applicable transaction is finalized. Customers often contact the Company following a transaction, e.g., with questions relating to the transaction or need for support, which necessitates, that the Company stores Personal Information relating to the customer for this period. The Company finds this to be in line with the original purpose, pursuant to which the Personal Information was processed.

If an individual customer requests further support or references the original transaction, Personal Information may be stored for an additional period, to enable the Company to provide the best customer experience and complete the transaction. The additional period is assessed on a case-by-case basis by the individual Employee. The employee processing the Personal Information shall be responsible for deleting the Personal Information when the additional period expires.

POTENTIAL CUSTOMERS

Personal Information relating to potential customers is kept for 2 years from the time point of contact is initiated. The Company has experienced that customer can have a prolonged decision process prior to conducting a transaction with the

Company, this necessitates that the Company stores and processes their Personal Information to potentially be able to support in the transaction process.

SUPPLIERS PARTNERS AND SIMILAR

Personal Information relating to suppliers, partners or similar is kept for 3 years following the conclusion of a transaction/partnership/agreement. The retention period is defined to enable warranty claims or support in accordance with customary statute of limitations.

EMPLOYEES

Personal Information received through a job application process (i.e. by way of job postings or unsolicited contact) is kept for 6 months following the receipt and 12 months following a consent from the data subject.

Personal Information received and processed in connection with the employment of an employee is kept for 5 years following the termination of the employment. The retention period is defined to enable the Company to settle any financial obligations and ensure documentation relating to the Employee's time at the Company including the period leading up to the termination/resignation of the Employee's contract.

See section 9 for further detail about employee rights.

EXEMPTIONS

Irrespective of the retention periods defined above, Personal Information may be kept for a shorter period, if it is deemed appropriate to delete the data sooner (i.e. due to the purpose being exhausted and/or Personal Information no longer needed).

Notwithstanding the periods defined above, all Personal Information relating to accounting or book-keeping (including documentation for expenses and similar) is kept in accordance with applicable law for a period of minimum 5 years.

Further, the Company has defined the following exemptions which – following an individual assessment – may result in longer retention periods than set out above:

- If processing is necessary pursuant to applicable law;
- If processing is necessary due to warranty claims, legal proceedings or similar;
- If processing is necessary due to rules governing liability to enable the Company to evidence certain matters of fact.

SECTION 9: PERSONAL INFORMATION RELATING TO EMPLOYEES

This section concerns the processing conducted by the Company of Personal Information relating to employees.

With the additions of the below rights and information all employees shall have the same rights as the Company's customers. The rights can be accessed through the Company's website as part of the Company's privacy notice. This includes, inter alia, an employee's right to access Personal Information relating to the employee.

PROCESSING AND PURPOSE

The Company Processes regular Personal Information such as contact information, photos, salary information, account details, social security numbers. The legal basis for processing is the General Data Protection Regulation (GDPR) Art. 6(1)(b)(c)(f), Article 87 and the Data Protection Act §§ 6 and 11.

The Company's purpose for processing Personal Information of employees is to establish and maintain and employment relationship including enhancing the work environment, career planning etc.

The Company processes regular special categories of Personal Information such as health information, biometric information, information on genetics, information on union affiliation (i.e. fagforeningsforhold). The legal basis for processing is the General Data Protection Regulation (GDPR) Art. 7 and 9(2)(a) and (b).

TRANSMISSION TO THIRD PARTIES

Personal Information relating to employees are only transmitted to third parties as required and when necessary. The transmission includes transmission to public authorities and municipalities.

Further, the Company have employed various third-party providers as data processors. This includes ADP for pay-roll management and Microsoft for IT-hosting. The Company have entered into data processing agreements with all data processors.

The Company offers its employees pension and insurance schemes, including health insurance. When required to deliver these services the Company may transfer Personal Information relating to an employee to providers of such schemes.

RETENTION OF EMPLOYEE PERSONAL INFORMATION

Personal Information relating to employees is deleted, when the Company's purpose for processing is exhausted or no longer valid. This will generally be 5 years following the termination/resignation of the employment.

Some Personal Information may be kept longer, if required by mandatory law.

SECTION 10: AUDIT AND CONTROL

The Company shall be required to maintain an appropriate catalogue of controls in ComplianceLog, a compliance management system. The controls shall be aimed at verifying and documenting compliance with this policy and any other documents intended to regulate, govern, or address the processing of Personal Information. This includes controls and audits of data processors, retention periods, technical and organizational security measures, risk assessments, training and Employee awareness and similar.