CYFERD

DATA PROTECTION POLICY

1. Scope

1.1 This '*Cyferd – Data Protection Policy*' (this "**Policy**") applies to the basis on how Cyferd Inc. ("**Cyferd**") (as Processor) will process Protected Data for a Customer (as Controller) in connection with Cyferd providing Access to the Cyferd Product to that Customer pursuant to the Agreement relating to that Customer (each such capitalized term and '*process*' as defined below). This Policy is made in connection with the provision by Cyferd Inc. ("**Cyferd**") of Access to the Cyferd Product to its customers (including those whose Access to the Cyferd Product is/ was procured through a Cyferd Partner) (in this Policy each a "**Customer**").

1.2 In this Policy the "**Agreement**" means, in respect of the Customer in question, the master services agreement known as '*Cyferd – MSA (A) – 1 August 2024*' entered into/ accepted by that Customer. The online version of the Agreement where accepted being found at https://cyferd.com/cyferdcomm/us.

1.3 This Policy is a Cyferd Policy and applies to, forms part of and is supplemental to the Agreement. The terms of Agreement shall apply to this Policy and are incorporated herein, mutatis mutandis, to this Policy.

1.4 For each Customer, this Policy together with the applicable Order Form, the Agreement, the other Cyferd Policies and any other applicable document that forms part of and/or is supplemental to the Agreement from time to time, applies to the subject matter of that Order Form and that Customer's Access to the Cyferd Product.

1.5 Unless otherwise noted or where the context otherwise requires, all capitalized terms used herein shall have the meanings set forth in the Agreement and the definitions document known as '*Cyferd – Definitions re MSA (A) – 1 August 2024*' (https://cyferd.com/cyferdcomm/us).

1.6 In addition, in this Policy the following words and expressions shall have the following meaning unless the context otherwise requires:

"**the Annexure**" the document annexed to this Policy at '*the Annexure*' which is an '*Overview of how the 'Cyferd Platform' operates*' as amended from time to time by Cyferd

"**Applicable Law**" means the following as applicable and binding on the party in question in connection with the Customer's Access to the Cyferd Product: (i) any law, legislation, regulation, byelaw or subordinate legislation in force from time to time; (ii) the common law and laws of equity as applicable to the parties from time to time; (iii) any binding court order, judgment or decree; or (iv) any applicable direction, policy, rule or order made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business

"**Article 46 Tools**" the tools provided for in Article 46 of the GDPR as mechanisms for safeguarding Protected Data being the subject matter of a ‘restricted’ Transfer (each an “**Article 46 Tool**”)

“**Controller**”

has the meaning given to that term in Data Protection Laws

“**Cyferd Rate Card**”

the ‘**Cyferd Rate Card**’ (https://cyferd.com/cyferdcomm/us) as the same may be amended from time to time by Cyferd

“**Data Protection Laws**”

means as applicable and binding on either party or the Customer in question’s Access to the Cyferd Product: (i) the GDPR; (ii) the Data Protection Act 2018 (being legislation in England and Wales); (iii) any laws which implement or supplement any such laws; and (iv) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing

“**Data Protection Losses**”

means all liabilities arising directly or indirectly from any breach or alleged breach of any of the Data Protection Laws or of this Policy, including all: (i) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); (ii) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (iii) compensation which is ordered by a court or Supervisory Authority to be paid to a Data Subject; and/or (iv) costs of compliance with investigations by a Supervisory Authority

“**Data Subject**”

has the meaning given to that term in Data Protection Laws

“**Data Subject Request**”

means a request made by a Data Subject to exercise any rights of Data Subjects under Chapter III of the GDPR in relation to any Protected Data

“**Dealing with Data Subject Requests Policy**”

as defined in **paragraph 8.3**

“**GDPR**”

means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time)

“**Hosting/ Data Storage Arrangements**”

as defined in **paragraph 9.2**

“**Hosting/ Data Storage Regions**”

the particular designated regions by Cyferd from time to time (comprising one or more Hosting/ Data Storage Territories) where Cyferd has a main hosting function (a Primary Datacenter Location) and a replicate/ back-up function (a

Secondary Datacenter Location) in respect of the Hosting/ Data Storage Arrangements (each such region a “**Hosting Data Storage Region**”)

“**Hosting/ Data Storage Territories**” and “**Hosting/ Data Storage Territory**” each as defined in **paragraph 9.2**

“**International Recipient**” means the organizations, bodies, persons and other recipients to which Transfers of the Protected Data are prohibited under **paragraph 9.1** without the applicable Customer’s prior written authorization

“**Lawful Safeguards**” means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time

“**List of Sub-Processors**” means the latest version of the list of Sub-Processors used by Cyferd, as amended from time to time by Cyferd, which as at Order Acceptance is available at https://cyferd.com/cyferdcomm/us

“**Overriding Principle**” (in respect of a Customer): (i) Cyferd will only ‘see’ or ‘have access to’ Customer Data of that Customer if that Customer discloses the same to Cyferd or where Cyferd is expressly entitled to/ required to ‘see’ or have access’ to the same under or in connection with the Agreement relating to that Customer; and (ii) (unless and to the extent that the Order Form(s) relating to that Customer and/or any other document that forms part of the Agreement relating to that Customer restrict the use case(s), App(s) and/or Feature(s) that the Customer is permitted to use (as an Access/Usage Parameter)) the Cyferd Product does not restrict the number of use cases and Apps that a Customer can make use of, and the extent of that Customer’s use is controlled by that Customer in its sole discretion

“**Permitted Auditor**” as defined in **paragraph 10.2**

“**Personal Data**” has the meaning given to that term in Data Protection Laws

“**Personal Data Breach”** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Protected Data

“**Pricing Terms (Data Protection)”** the applicable work shall be calculated and priced by Cyferd (at its sole discretion): (i) using the cheapest daily rate amount (plus applicable Taxes) set out in the Cyferd Rate Card; or (ii) in accordance with the **Dealing with Data Subject Requests Policy** (if and where it contains a pricing structure for the applicable work for the purposes of this Policy); or (iii) any combination of (i) or (ii), and such price could (as applicable) take into account time spent, materials used, expenses incurred, App Usage and/or any market fee or pricing in respect of the same

"**Primary Datacenter Location**" as defined in **paragraph 9.2.1**

"**processing**" has the meaning given to that term in Data Protection Laws (and related terms such as "**process**", "**processes**" and "**processed**" have corresponding meanings)

"**Processing Instructions**" as defined in **paragraph 5.1.1**

"**Processor**" has the meaning given to that term in Data Protection Laws

"**Protected Data**" means Personal Data in the Customer Data

"**Relevant Territory**" a country or territory or those countries or territories where (as a result of local laws or local restrictions) Cyferd cannot use its standard hosting of/ data storage in connection with the Cyferd Product and has implemented separate or enhanced arrangements for the hosting of/ data storage in connection with the Cyferd Product to comply with/ accommodate such local laws or local restrictions (such arrangements being set out in a supplemental document or addendum to Cyferd's **Hosting Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended from time to time by Cyferd) and/or Cyferd's **Storage of and Access to Customer Data Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended from time to time by Cyferd) as applicable) (and "**Relevant Territories**" shall be construed accordingly)

"**Secondary Datacenter Location**" as defined in **paragraph 9.2.1**

"**Site Reliability Engineering**" the IT operations function (the Hosting/Data Storage Arrangements, quality assurance and security) in connection with the Cyferd Product and being specifically focused making sure production runs in respect of the same

"**SRE Personnel**" those persons employed by or contracted to: (i) Cyferd and/or any of its Affiliates; or (ii) the Sub-Processor in question (as the case may be), who deal with the Site Reliability Engineering (or any part of it) (and "**Cyferd's SRE Personnel**" and a "**Sub-Processor's SRE Personnel**" shall be construed accordingly)

"**Standard Contractual Clauses**" means 'Standard Contractual Clauses' for the transfer of Protected Data to International Recipient(s) pursuant to the GDPR (being an Article 46 Tool)

“**Sub-Processor**” means a Processor engaged by Cyferd or by any other Sub-Processor for carrying out processing activities in respect of the Protected Data on behalf of the Customer in question

“**Supervisory Authority**” means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws

“**Transfer**” bears the same meaning as the word ‘transfer’ in Article 44 of the GDPR (and related terms such as “**Transfers**”, “**Transferred**” and “**Transferring**” have corresponding meanings)

2. Last Updated

This Policy was last updated on 1 August 2024. For previous versions of this Policy see https://cyferd.com/cyferdcomm/us.

3. Changes to this Policy

3.1 ***For any person who is not a Customer at the time of such posting*** - Cyferd shall, at its absolute discretion, be entitled to amend this Policy or any part of it by posting an updated version of this Policy at https://cyferd.com/cyferdcomm/us and such updates will be effective upon such posting or, if later, the ‘Last Updated’ date specified in such updated version of this Policy.

3.2 ***For any person who is a Customer at the time such Update Notification is made*** –Cyferd may at its absolute discretion make, and notify the Customer of, updated versions of this Policy by notifying the Customer of any such Update(s) by way of Update Notification in accordance with the Agreement. Such Update(s) will be effective in respect of the Customer in question in accordance with the applicable provisions of the Agreement.

3.3 If Cyferd makes any amendments to this Policy, it will change the ‘Last Updated’ date in **paragraph 2** above in such updated version of this Policy.

4. Processor and Controller

4.1 The parties agree that, for the Protected Data, the Customer shall be the Controller and Cyferd shall be the Processor. Nothing in the Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

4.2 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorization of all relevant Controllers to instruct Cyferd to process the Protected Data in accordance with this Policy and the Agreement.

4.3 Cyferd shall process Protected Data in compliance with:

4.3.1 the obligations of Processors under Data Protection Laws in respect of the performance of its obligations under this Policy; and

4.3.2 the terms of the Agreement.

4.4 The Customer shall ensure that it and each of its Authorized Users shall at all times comply with:

4.4.1 all Data Protection Laws in connection with the processing of Protected Data, the Customer’s Access to the Cyferd Product (and each part) and the exercise and performance of its respective rights and obligations under the Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

4.4.2 the terms of the Agreement.

4.5 The Customer warrants, represents and undertakes, that at all times:

4.5.1 the processing of all Protected Data in accordance with the Agreement shall comply in all respects with Data Protection Laws, including in terms of its collection, use and storage;

4.5.2 fair processing and all other appropriate notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Data Protection Laws in connection with all processing activities in respect of the Protected Data that may be undertaken by Cyferd and its Sub-Processors in accordance with the Agreement;

4.5.3 the Protected Data is accurate and up to date;

4.5.4 it shall establish and maintain adequate security measures to safeguard the Protected Data in its possession or control (including from unauthorized or unlawful destruction, corruption, processing or disclosure) and maintain complete and accurate backups of all Protected Data provided to Cyferd (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by Cyferd or any other person;

4.5.5 all instructions given by it to Cyferd in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

4.5.6 it has undertaken due diligence in relation to Cyferd's processing operations and commitments and it is satisfied (and at all times it continues to have Access to the Cyferd Product remains satisfied) that:

4.5.6.1 Cyferd's processing operations are suitable for the purposes for which the Customer proposes to use the Cyferd Product and (in doing so) engage Cyferd to process the Protected Data;

4.5.6.2 the technical and organizational measures set out in the **Storage of and Access to Customer Data Policy** ensure a level of security appropriate to the risk in regard to the Protected Data as required by Data Protection Laws; and

4.5.6.3 Cyferd has sufficient expertise, reliability and resources to implement technical and organizational measures that meet the requirements of Data Protection Laws.

4.6 The Customer agrees and acknowledges the Overriding Principle.

5. Instructions and details of processing

5.1 Insofar as Cyferd processes Protected Data on behalf of the Customer, Cyferd:

5.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in the Agreement (including with regard to Transfers of Protected Data to any International Recipient) ("**Processing Instructions**");

5.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

5.1.3 shall promptly inform the Customer if Cyferd becomes aware of a Processing Instruction that, in Cyferd's opinion, infringes Data Protection Laws, provided that:

5.1.3.1 this shall be without prejudice to **paragraphs 4.4** and **4.5**; and

5.1.3.2 to the maximum extent permitted by Applicable Law, Cyferd shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Processing Instructions following the Customer's receipt of the information required by this **paragraph 5.1.3**.

5.2 The Customer agrees that:

5.2.1 Cyferd (and each Sub-Processor) is not obliged to undertake any processing of Protected Data that Cyferd believes infringes any of the Data Protection Laws and shall not be liable (or subject to any reduction or set-off of any Fees and/or other fees or monies payable to Cyferd in connection with the Agreement) to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under the Agreement as a result of not undertaking any processing in such circumstances; and

5.2.2 without prejudice to any other right or remedy of Cyferd, in the event the Customer has not resolved any Processing Instruction notified to it under **paragraph 5.1.3** such that it is lawful in Cyferd's opinion within 7 (seven) days of such notification then the Customer shall be deemed to be in material breach of the Agreement which is not remediable and Cyferd may terminate the Agreement in accordance with its terms.

5.3 The Customer shall be responsible for ensuring all of its Authorized Users read and understand Cyferd's **Privacy Policy** (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended from time to time by Cyferd).

5.4 The Customer acknowledges and agrees that the execution of any computer command to process (including deletion of) any Protected Data made in connection with the Access to the Cyferd Product and the Professional Services (or any of them) by any of its Authorized Users will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons, including as set out in the Documentation). The Customer shall ensure that its Authorized Users do not execute any such command unless authorized by the Customer (and by all other relevant Controller(s)) and acknowledges and accepts that if any Protected Data is deleted pursuant to any such command Cyferd is under no obligation to seek to restore it.

5.5 The duration processing of the Protected Data by Cyferd under the Agreement, the nature and purpose of such processing, the types of Personal Data and categories of Data Subjects so processed are further specified in **the Schedule** to this Policy.

6. Technical and organizational measures

6.1 Cyferd shall implement and maintain technical and organizational measures:

6.1.1 in relation to the processing of Protected Data by Cyferd, as set out in/ referred to in the **Storage of and Access to Customer Data Policy**, the **Hosting Policy** and the **Annexure**; and

6.1.2 (having strict regard to the provisions of the **Storage of and Access to Customer Data Policy**, the Overriding Principle to assist the Customer insofar as is possible (taking into account the nature of the processing) in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data, in each case at the Customer's cost, the price for which shall be calculated in accordance with the Pricing Terms (Data Protection). The parties have agreed that (taking into account the nature of the processing) Cyferd's compliance with **paragraph 8.1** shall constitute Cyferd's sole obligations under this **paragraph 6.1.2**.

6.2 During the period in which Cyferd processes any Protected Data, the Customer shall be entitled to undertake a documented assessment of whether the security measures implemented in accordance with **paragraph 6.1** are sufficient to protect the Protected Data against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access to the extent required by Data Protection Laws in the circumstances. The Customer shall promptly notify Cyferd of full details of any additional measures the Customer believes are required as a result of the assessment. The Customer acknowledges that Cyferd provides a commoditized one-to-many service and the needs or assessments of other customers may differ. Cyferd shall not be obliged to implement any further or alternative security measures and if Cyferd does not so implement any further or alternative security measures then the Customer's sole recourse in respect of the same is to terminate the Agreement immediately by giving notice in writing to Cyferd within 30 (thirty) days of Cyferd's decision not to implement any further or alternative security measures, such termination to take effect on the expiry of the notice. In the event of such valid termination by the Customer under this **paragraph 6.2** then (given the warranties, representations and undertakings set out in **paragraph 4.5**) applicable clauses of the Agreement shall apply.

7. Using staff and other Processors

7.1 Subject to **paragraph 7.2**, Cyferd shall not engage (nor permit any other Sub-Processor to engage) any Sub-Processor for carrying out any processing activities in respect of the Protected Data in connection with the Agreement without the Customer's prior written authorization. The Customer shall not unreasonably object to any new Sub-Processor (or any change to any of the Sub-Processors).

7.2 The Customer:

7.2.1 authorizes the appointment of each of the Sub-Processors identified on the List of Sub-Processors as at Order Acceptance; and

7.2.2 authorizes the appointment of each Sub-Processor (or any change to any of the Sub-Processors) identified on the List of Sub-Processors. The Customer's right to object to the appointment of a new Sub-Processor (or any change to any of the Sub-Processors) following the relevant Update Notification introducing that change may be exclusively exercised by terminating the Agreement.

7.3 Cyferd shall:

7.3.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure each Sub-Processor is appointed under a written contract containing materially the same obligations as under **paragraphs 4** to **14** (inclusive) (including those obligations relating to sufficient guarantees to implement appropriate technical and organizational measures); and

7.3.2 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

7.4 Cyferd shall ensure that its personnel/ its Affiliate's personnel engaged in the processing of Protected Data (including Cyferd's SRE Personnel) are informed of the confidential nature of the Protected Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements (in favor of Cyferd).

8. Assistance with compliance and Data Subject rights

8.1 Cyferd shall refer all Data Subject Requests (that expressly relate to the Customer and any applicable Protected Data) it receives to the Customer without undue delay. The Customer shall pay Cyferd for all work, time, costs and expenses incurred by Cyferd or any Sub-Processor(s) in connection with such activity, calculated in accordance with the Pricing Terms (Data Protection).

8.2 Cyferd shall provide such commercially reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to Cyferd and having strict regard to the Overriding Principle) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

8.2.1 security of processing;

8.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

8.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

8.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay Cyferd for all work, time, costs and expenses incurred by Cyferd or any Sub-Processor(s) in connection with providing the assistance in this **paragraph 8.2**, calculated in accordance with the Pricing Terms (Data Protection).

8.3 Cyferd may from time to time have another Cyferd Policy which is/ will be known as the '*Cyferd - Dealing with Data Subject Requests Policy*' (https://cyferd.com/cyferdcomm/us) (being a Cyferd Policy and as amended from time to time by Cyferd) that specifically deals with dealing with Data Subject Requests that expressly relate to the Customer and any applicable Protected Data (the "**Dealing with Data Subject Requests Policy**"). The **Dealing with Data Subject Requests Policy** may include provisions that confirm what the assistance referred to in **paragraph 8.2** shall include and/or comprise and/or the scope of any such assistance. The **Dealing with Data Subject Requests Policy** may also contain the pricing structure for Cyferd providing the assistance referred to in **paragraph 8.2**.

9. International data Transfers

9.1 Subject to **paragraphs 9.2**, **9.3** and **9.6**, Cyferd shall not Transfer any Protected Data without the Customer's prior written authorization except where required by Applicable Law (in which case the provisions of **paragraph 5.1** shall apply).

9.2 (Subject to any special hosting and/or data storage arrangements agreed with the Customer in the Order Form(s) under the Agreement) those countries and territories which are applicable to the then current hosting and/or data storage arrangements for the Cyferd Product (without which the Customer could not Access the Cyferd Product) as provided for/ referred to in **the Annexure**, the **Hosting Policy** and (if applicable) the **Storage of and Access to Customer Data Policy** (such hosting and/or data storage arrangements being the "**Hosting/ Data Storage Arrangements**") which include**:**

9.2.1 any country or territory that the **Hosting Policy** provides is a then country or territory where the Cyferd Product is then currently hosted (whether as a main hosting function (each such main hosting function location being a "**Primary Datacenter Location**") or a replicate and back-up function (each such replicate and back-up function location being a "**Secondary Datacenter Location**"); and/or

9.2.2 (where the Customer is based in a Relevant Territory and/or needs to Access the Cyferd Product from a Relevant Territory) that Relevant Territory or each of the applicable Relevant Territories (as the case may be),

(such countries and territories being together the "**Hosting/ Data Storage Territories**" and each a "**Hosting/ Data Storage Territory**"). The Transfer of Protected Data will occur between the applicable Hosting/ Data Storage Territories in a particular Hosting/ Data Storage Region as part of the Hosting/ Data Storage Arrangements. For example, if an Authorized User (based in the United Kingdom or Spain for the purposes of this example) of the Customer (being based in France for the purposes of this example) executes a computer command to process any Protected Data as part of/ during the Customer's Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)) (being a Processing Instruction) then the applicable Primary Datacenter Location and the applicable and corresponding Secondary Datacenter Location will be the applicable Hosting/ Data Storage Arrangements for the Customer and the result of that Processing Instruction will be: (i) recorded (in two separate copies) as part of the main current hosting arrangements for the Cyferd Product in the applicable Primary Datacenter Location and (ii) replicated (as an additional copy) as part of the replication/ back-up current hosting arrangements for the Cyferd Product in the applicable and corresponding Secondary Datacenter Location.

9.3 The Customer hereby authorizes Cyferd (or any Sub-Processor) to Transfer any Protected Data for the purposes referred to in **paragraph 5.5** to any International Recipient(s) in accordance with **paragraph 9.4**, provided all Transfers of Protected Data by Cyferd (or any Sub-Processor) to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Lawful Safeguards and in accordance with Data Protection Laws and the Agreement. The provisions of the Agreement (including this Policy) shall constitute the Customer's instructions with respect to Transfers in accordance with **paragraph 5.1.1**.

9.4 Cyferd (and its Sub-Processors) may only Transfer the Protected Data to (or process Protected Data in) the following countries and territories: (i) the Hosting/ Data Storage Territories (or any of them), (ii) any country or territory where the Customer (itself and/or via its Administrator and/or its Authorized Users) executes a computer command to process any Protected Data as part of/ during the Customer's Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)) (being a Processing Instruction) where the same amounts to a Transfer, the extent of which is controlled by the Customer in its sole discretion; (iii) any country or territory where any of Cyferd's SRE Personnel and/or any of a Sub-Processor's SRE Personnel executes a computer command to process any of the Customer's Protected Data as part of the Site Reliability Engineering where the same amounts to a Transfer; and (iv) (notwithstanding (i) and (iii) above) any country or territory where a Sub-Processor executes a computer command to process any of the Customer's Protected Data as part of the provision of its sub-processing services/ services to Cyferd in connection with the Customer's Access to the Cyferd Product where the same amounts to a Transfer). Where applicable, further detail in this regard is contained in **the Annexure**, the **Hosting Policy**, the **Storage of and Access to Customer Data Policy** and/or the **Privacy Policy.**

9.5 The Lawful Safeguards employed in connection with Transfers pursuant to **paragraph 9.2** shall be as follows: Cyferd will (where applicable) undertake a transfer risk assessment or a transfer impact assessment prior to making a 'restricted' Transfer to verify, on a case-by-case basis, if the law or practice of the third county in question impinges on the effectiveness of the Article 46 Tool to be used and/or to see if there is a then current '*adequacy decision*' or '*adequacy regulation*' stating that the specific International Recipient or third country in question provides an adequate level of protection in respect of the proposed 'restricted' Transfer. Where possible, Cyferd will use applicable Standard Contractual Clauses as the mechanism for safeguarding Protected Data that is the subject matter of a 'restricted' Transfer; or, where not possible, the use any of the other Article 46 Tools **PROVIDED THAT**:

9.5.1 Where the applicable Article 46 Tool on its own would not (in Cyferd's opinion (having regard to the transfer risk assessment/ transfer impact assessment)) provide sufficient safeguards, Cyferd will (if and to the extent required) implement supplementary measures/ extra steps and protections, which may be standard contracts clauses, data privacy framework, organizational and/or technical, to bring protections up to the level required by law.

9.6 The Customer acknowledges that due to the nature of cloud services, the Protected Data may be Transferred to other geographical locations in connection with the Customer's Access to the Cyferd Product further to access and/or computerized instructions initiated by Authorized Users. The Customer acknowledges that Cyferd does not control such processing and the Customer shall ensure that Authorized Users (and all others acting on its behalf) only initiate the Transfer of Protected Data to other geographical locations if Lawful Safeguards are in place and that such Transfer is in compliance with all Applicable Laws.

10. Information and audit

10.1 Cyferd shall maintain, in accordance with Data Protection Laws binding on Cyferd, written records of all categories of processing activities carried out on behalf of the Customer. The Customer will already have access to the data logs relating to its Tenancy(ies). Cyferd will have access to 'Platform data logs' in respect of the Cyferd Product part of which will relate to the Customer's Tenancy(ies)/ generic 'Platform' activity relevant to all Customers and part of which will relate to other Customers' Tenancies

10.2 On request, Cyferd shall provide the Customer (or a Permitted Auditor mandated by the Customer) with a copy of the third-party certifications and audits to the extent made generally available to its customers. A "**Permitted Auditor**" is an independent third-party auditor who specializes in data protection audits and who has (in Cyferd's sole opinion (acting reasonably)) suitable experience in dealing with PaaS providers and how PaaS providers act as Processors in providing such PaaS and whose identity has been approved by Cyferd (acting reasonably) in writing for such purpose; it being reasonable for Cyferd to reject any third-party auditor for this purpose who is a competitor of Cyferd, who is an Affiliate of or associated or connected with any such competitor(s), who is known to be a supplier to, contractor of or representative of any such competitor(s) or who has a conflict of interests. A Permitted Auditor shall be required to enter into a separate confidentiality agreement in favor of Cyferd in a form to Cyferd's satisfaction in this regard.

10.3 Notwithstanding the generality of **paragraph 10.2**, any information provided to the Customer arising from, in connection with or relating to any information request or audit or inspection in connection with **paragraph 10.2** or otherwise shall be confidential to Cyferd and shall be Confidential Information as defined in the Agreement, and shall be subject to the Customer's confidentiality obligations in the Agreement (*Cyferd's Confidential Information*). Where such audit, inspection or information request is for information over and above that referred to in **paragraph 10.2** and Cyferd is willing and able to accommodate the same/ is required under Data Protection Laws to accommodate the same then:

10.3.1 such audit, inspection or information request shall be reasonable, limited to information in Cyferd's possession or control and is subject to the Customer giving Cyferd reasonable (and in any event at least 60 (sixty) days') prior notice of such audit, inspection or information request;

10.3.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third-party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure Cyferd is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this **paragraph 10.3**);

10.3.3 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of Cyferd;

10.3.4 the duration of any audit or inspection shall be limited to 1 (one) Business Day;

10.3.5 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and the price for Cyferd's costs, expenses, work and time incurred in connection with such audit or inspection or responding to such information request shall be calculated in accordance with the Pricing Terms (Data Protection);

10.3.6 the Customer's rights under this **paragraph 10.3** in connection with such audit, inspection or information request may only be exercised once in any consecutive 12 (twelve) month period, unless otherwise required by a Supervisory Authority;

10.3.7 the Customer shall promptly (and in any event within 1 (one) Business Day) report to Cyferd any non-compliance identified by such the audit, inspection or release of information;

10.3.8 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any Permitted Auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of Cyferd while conducting any such audit or inspection; and

10.3.9 this **paragraph 10.3** is subject to **paragraph 10.4**.

10.4 The Customer acknowledges and accepts that relevant contractual terms agreed with Sub-Processor(s) may mean that Cyferd or the Customer may not be able to undertake or facilitate an information request or audit or inspection of any or all Sub-Processors in connection with **paragraph 10.2** or otherwise and:

10.4.1 (if any) the Customer's rights undertake or facilitate an information request or audit or inspection of any or all Sub-Processors in connection with **paragraph 10.2** or otherwise shall not apply to the extent inconsistent with relevant contractual terms agreed with Sub-Processor(s); and

10.4.2 **paragraphs 7.3.1** and **10.2** shall be construed accordingly.

11. Breach notification

11.1 Subject to **paragraph 11.2**, in respect of any Personal Data Breach, Cyferd shall, without undue delay:

11.1.1 notify the Customer of the Personal Data Breach; and

11.1.2 provide the Customer with details of the Personal Data Breach.

11.2 In respect of its Access to the Cyferd Product, the Customer (via its Administrator) is responsible for giving, managing and maintaining its Authorized Users' Access by setting up its Authorized User Accounts.. The Customer shall, without undue delay:

11.2.1 notify Cyferd of any Personal Data Breach, security breach or failure, unauthorized access or other fact matter or circumstance that prejudice(s) the security of the Customer's Tenancy(ies) (or any of them) in respect of any Authorized User Account and/or the Customer's Authentication Set Up;

11.2.2 provide Cyferd with details of the same.

Given the Overriding Principle, the Customer agrees and acknowledges that Cyferd will not know about any of the matters referred to in **paragraph 11.2.1** unless and until the Customer informs Cyferd of the same. The Customer further agrees and acknowledges that Cyferd may need to, and if so, shall notify: (i) other applicable Customers of the same where it could impact the Tenancies (or any of them) of other Customers and/or (ii) any applicable Sub-Processors. Where and to the extent possible, Cyferd shall make any such notification(s) on an anonymized basis. In any event the Customer hereby expressly consents to any such notification(s) being made by Cyferd.

12. Deletion of Protected Data and copies

Following the end of the Term of the Agreement or, if such Agreement is terminated earlier (in whole or in part), the applicable date of termination the Supplier shall dispose of the applicable Protected Data in accordance with its obligations under the Agreement and the **Storage of and Access to Customer Data Policy**). Cyferd shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with the Agreement.

13. Compensation and claims

13.1 Subject to the Agreement, Cyferd shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with the Agreement:

13.1.1 only to the extent caused by the processing of Protected Data under the Agreement relating to the Customer and directly resulting from Cyferd's breach of the Agreement; and

13.1.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of the Agreement by the Customer (including in accordance with **paragraph 5.1.3.2**) and/or otherwise contributed to or caused by the Customer and/or any of its Authorized Users.

13.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with the Agreement or the Customer's Access to the Cyferd Product, it shall promptly provide the other party with notice and full details of such claim.

13.3 The parties agree that the Customer shall not be entitled to claim back from Cyferd any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify or otherwise compensate Cyferd in accordance with the Agreement and/or to the extent Cyferd has no liability for the same under the Agreement.

13.4 This **paragraph 13** is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

13.4.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

13.4.2 that it does not affect the liability of either party to any Data Subject.

14. Survival

This Policy shall survive termination (for any reason) or expiry of the Agreement with the Customer in question and continue until no Protected Data in relation to that Customer remains in the possession or control of Cyferd or any Sub-Processor, except that **paragraphs 12** to **14** (inclusive) shall continue indefinitely.

15. Data protection contact

Cyferd's '*Data Protection Officer*' may be contacted at pivacy@cyferd.com.

16. Failure to comply with/ breach of this Policy by the Customer

Without limiting anything else herein or in the Agreement, if Customer fails to comply with and/or otherwise breaches any term(s) of this Policy, then such failure to comply/breach will be considered to be a material breach by the Customer of the Agreement, and for which Cyferd shall be entitled to, without limitation, exercise all available rights and remedies under the Agreement.

[End of Policy]

THE SCHEDULE

Subject-matter of processing:

The Customer in question's Access to the Cyferd Product including particular:

- The Hosting Services; and
- The Database Services.

Duration of the processing:

Subject to **paragraph 14**, in respect of a Customer the duration of the processing of that Customer's Protected Data by Cyferd is the Term (of the Agreement relating to that Customer) or, if such Agreement is terminated earlier (in whole or in part), the applicable date of termination.

Frequency of the processing:

Continuous basis depending on a Customer's use of its Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)).

Nature and purpose of the processing:

The processing of a Customer's Protected Data by Cyferd under the Agreement relating to that Customer shall (having strict regard to the Overriding Principle) be for the following purposes (such purposes being Processing Instructions given to Cyferd by that Customer):

- processing in accordance with the rights and obligations of the parties under the Agreement relating to that Customer;
- processing to provide that Customer's Access to the Cyferd Product (including the Hosting/ Data Storage Arrangements);
- processing to comply with other reasonable instructions provided by that Customer where such instructions are consistent with the terms of the Agreement relating to that Customer; and
- processing as reasonably initiated, requested or instructed by:
    - that Customer's Authorized Users in connection with their use of that Customer's; and/or
    - that Customer in connection with its,

  Access to the Cyferd Product in each case in a manner consistent with the Agreement relating to that Customer.

Type of Personal Data:

A Customer may upload, submit, enter and/or otherwise process (itself and/or via its Administrator and/or its Authorized Users) Protected Data as part of/ during that Customer's Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)), the extent of which is controlled by that Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects in relation to that Customer (where the same are natural persons):

- Administrators;
- Authorized Users;
- Prospects, customers, clients, suppliers, contractors, sub-contractors, consultants, freelancers, brokers, other service providers, agents, distributors, referrers, introducers and/or business partners of or to that Customer and/or any of its Affiliates;
- Members, shareholders and/or partners of that Customer and/or any of its Affiliates;
- Investors, lenders, funders, financiers, creditors, security or collateral providers, guarantors and/or sureties of or to that Customer and/or any of its Affiliates;
- Advisors, professional advisors, other professional service providers, insurers;
- Employees, directors, officers and/or workers of any of the foregoing; and/or
- Employees, directors, officers and/or workers of that Customer and/or any of its Affiliates.

Categories of Personal Data:

A Customer may upload, submit, enter and/or otherwise process (itself and/or via its Administrator and/or its Authorized Users) Protected Data as part of/ during that Customer's Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)), the extent of which is controlled by that Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First, last and any middle names
- Title
- Position
- Employer
- Contact information (company, email, phone, business address, home address, next of kin and such information relating to the next of kin)
- ID data
- Professional life data
- Personal life data
- Localization data

Special categories of Personal Data:

A Customer may input, upload, submit, enter and/or otherwise process (itself and/or via its Administrator and/or its Authorized Users) special categories (within the meaning of Article 9 of the GDPR) of Protected Data as part of/ during that Customer's Access to the Cyferd Product (or any part of it including any App(s) and Feature(s)), the extent of which is controlled by that Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or Personal Data which is or contains genetic data, biometric data, for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or any other form of special categories of Personal Data

THE ANNEXURE

There is annexed hereto an '*Overview of how the 'Cyferd Platform' operates*'.

This document provides an overview of how the Cyferd Platform operates and is intended to be supplemental to and clarify some of the content of the *'Cyferd - Data Protection Policy'*, the *'Cyferd – Hosting Policy'*, the *'Cyferd - Privacy Policy'* and the *'Cyferd – Storage of and Access to Customer Data Policy'*.

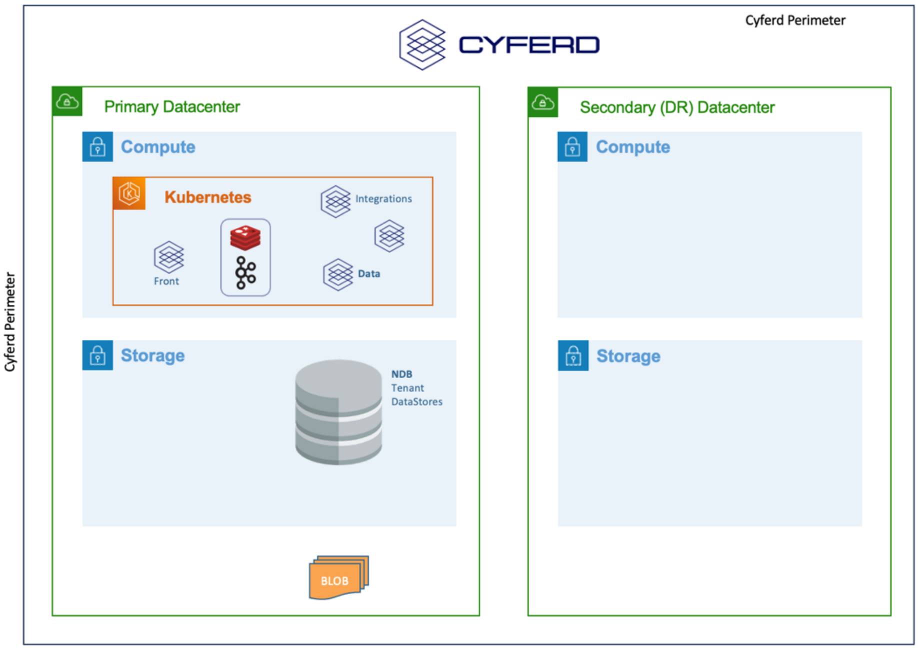
In this document "**Administrator**", "**Access**", "**Authorized User**", "**Customer Data**", "**Cyferd Product**", "**Tenancy**", "**Tenancies**", "**Tenancy(ies)**" have the meanings given to them the definitions document known as '*Cyferd – Definitions re MSA (A) – 1 August 2024*' (https://cyferd.com/cyferdcomm/us).

In this document "**Customer**" has the same meaning given to it in the applicable policy referred to above.

In this document "**Cyferd Platform**" has the same meaning as the Cyferd Product.

Cyferd Perimeter

The "**Cyferd Perimeter**" describes the boundaries of the Cyferd Platform, within which Cyferd Inc. ("**Cyferd**") takes responsibility to provide service to Customers (namely Access to the Cyferd Platform via its Tenancy(ies)) by using and managing many technologies deployed in tiered and secured network segments, operating in several Cyferd-managed locations.

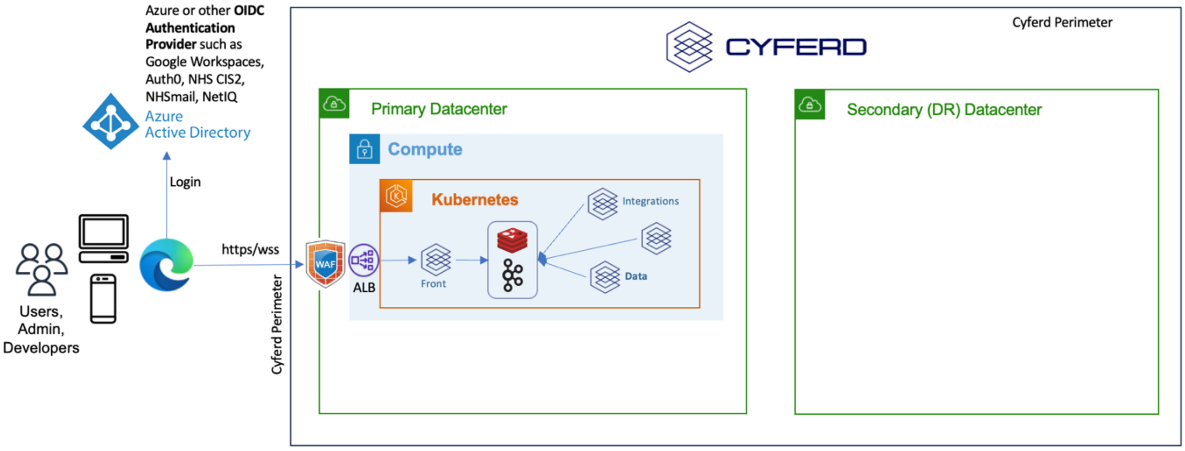


Here we can see that there are two Datacenters, implemented in different locations: the Primary Datacenter is where service is primarily delivered from, containing a 'compute' segment where the Cyferd Platform microservices operate in a Kubernetes cluster, and a 'storage' segment where the Customer Data (in respect of each Tenancy) and other data is stored; the Secondary Datacenter contains similar infrastructure that is maintained in a state of readiness to resume customer service in case (albeit very remote possibility) the Primary Datacenter becomes inaccessible or unsafe to use.

All services *outside* the Cyferd Perimeter are the responsibility of the Customer in question to provide, e.g. Authorized User authentication, and access to other datasources.

Ingress

The Cyferd Perimeter has only one Ingress for any Tenancy. Whether using an HTML5 compliant browser from a desktop (Windows, MacOS) or from a mobile device (iOS, iPadOS, Android), the Cyferd Mobile clients for Android/iOS, or programmatic interactions with the Cyferd Platform from another solution, all traffic is encrypted in transit, and terminated at the edge of the Cyferd Perimeter.



When a Customer's Authorized User browses to that Customer's Tenancy at https://tenant.cyferd.cloud/ the traffic traverses a *Web Application Firewall* (WAF) that performs validation of well-formed https requests and passes it on to an *Application Load Balancer* (ALB) that terminates the Transport Layer Security (TLS aka SSL) encrypted connection before forwarding the user request to a front-end Cyferd Platform microservice running within the Kubernetes cluster.

The initial response to attempting to connect is to redirect the Authorized User to the Authentication Provider that is configured for that Customer's Tenancy. Cyferd requires that the Customer supplied or approved Authentication Provider supports Open ID Connect (OIDC) to provide the authenticated Authorized User's identity to the Cyferd Platform. Popular OIDC Authentication Providers include Microsoft Azure Entra ID, Google Workspaces, Okta/Auth0, ADFS, and several niche providers such as NHS CIS2 and NHSmail (ADFS) are also supported.

The Customer is responsible for providing the authentication service for its Authorized Users.

Upon successful authentication and redirection to the Customer's Tenancy, a 'session' is established and traffic between the browser and the Cyferd Platform continues using a Secured Websocket. Data in transit through the Cyferd Perimeter is encrypted.

Programmatic interactions with the Cyferd Platform follow the same path of connectivity, however authentication may use an API Token that is created and managed within the Tenancy by an appropriately authorized Authorized User, and a RESTful API is supported instead of the Websocket.

Compute & Storage

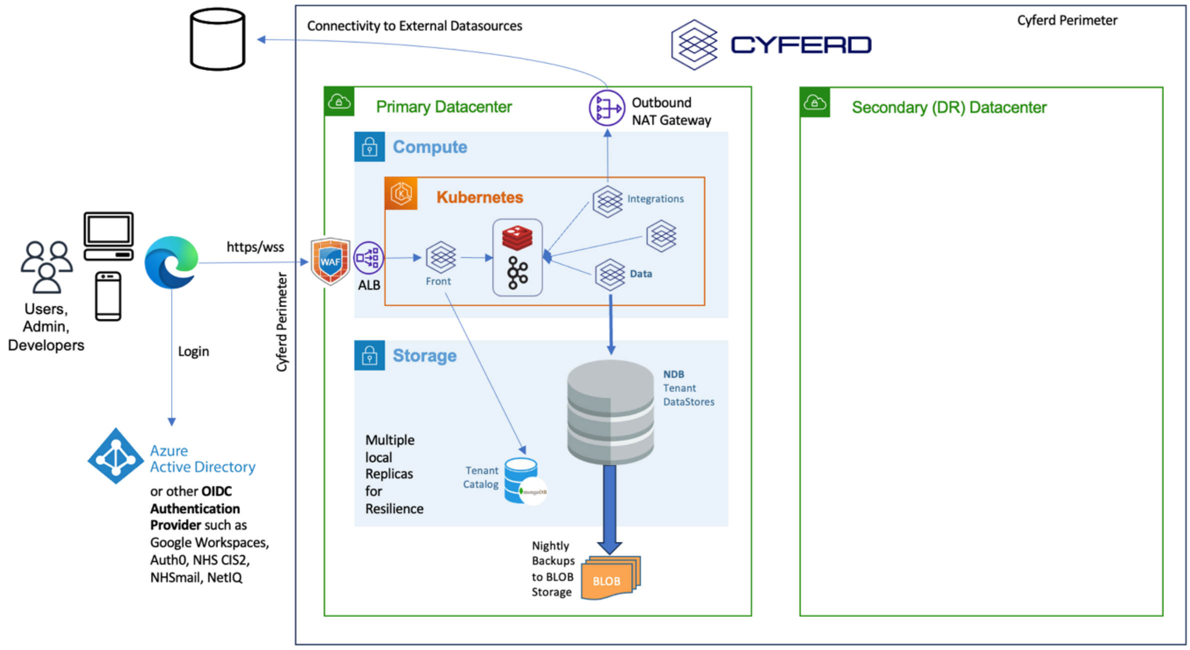
The Cyferd Platform is *multi-tenant*, meaning service to many Tenancies is delivered from shared infrastructure; individual Tenancies do not have individual installations.

Tenant Catalog

All Customers are described in the *Tenant Catalog*, which distinguishes multiple Tenancies by their HTTP Origin **tenant.cyferd.cloud** as used when connecting to the Cyferd Platform. Details in the *Tenant Catalog*, for each Customer (per Tenancy), include:

- the OIDC *Authentication Provider* properties:
  - Issuer Base URL
  - Client ID
  - Client Secret
- Identification of the Administrator of that Customer (*Super Users*) which must be valid identities provided by the *Authentication Provider* above
- *DataStore* properties (for several database technologies used by the Cyferd Platform
  - Database Name
  - Credentials
  - Optional URI if hosted in an irregular location
- *BLOB Storage* properties (used for uploaded *Documents*/*Images* and Backups)
  - Storage Type
  - Bucket Identifier
  - Access Key
  - Access Secret
  - Optional Region if in an irregular location

Cyferd manages the availability of Customer Data of a Customer (for that Customer's Tenancy(ies) in question) within the Cyferd Perimeter.


Connectivity to External Datasources
CYFERD
Cyferd Perimeter
Primary Datacenter
Outbound NAT Gateway
Secondary (DR) Datacenter
Compute
Kubernetes
Integrations
Front
Data
WAF
ALB
https/wss
Users, Admin, Developers
Login
Cyferd Perimeter
Storage
NDB Tenant DataStores
Multiple local Replicas for Resilience
Tenant Catalog
Nightly Backups to BLOB Storage
BLOB
Azure Active Directory
or other OIDC Authentication Provider such as Google Workspaces, Auth0, NHS CIS2, NHSmail, NetIQ

Compute

Authorized User interactions are enqueued to a pair of components (*Kafka & Redis*) which Cyferd calls "**Rex**" that provide loose coupling and horizontal scalability of the Cyferd Platform microservices.

Each microservice reads specific classes of work from Rex, and either provides a direct service (e.g. data manipulation, notification delivery) or interacts with another resource to query, modify or create data before responding to Rex.

For example (in respect of a Customer and each of that Customer's Tenancies):

- the **Front-End** microservice is the point that Authorized User interactions are submitted through, manages *User Session*, provides *Websocket* connectivity, and submits work to Rex. It also provides the response from Rex to the Authorized User through the *Websocket*.
- the **Data** microservice performs almost all interactions with that Customer's configured *DataStores* (for that Customer's Tenancy in question) – to search, list, modify, create, or delete data.
- the **Channels** microservice performs delivery of *Messages* to Authorized Users as *Mobile Notifications*, *Emails*, and within the Cyferd Platform user interface (for that Customer's Tenancy in question).
- The **Integrations** microservice provides connectivity to datasources or microservices *outside* the Cyferd Perimeter, as configured within that Customer's Tenancy in question, e.g. *Foreign Currency Exchange Rates*, *User Properties* in an external directory.
  Access to publicly accessible datasources is via an *Egress NAT Gateway* on the Cyferd Perimeter; access to private datasources inside the Customer's own '*Perimeter*' requires deployment of the *Cyferd Remote Agent* inside that '*Perimeter*' to implement a *Tunnel* that provide a network access path to those datasources.
- Other microservices perform a variety of utility functions within the Cyferd Platform. Cyferd may, in respect of the Cyferd Platform, redistribute work amongst existing or new microservices and add further optional capabilities at any time without obligation or notification.

Storage

The Cyferd Platform uses several technologies to store managed data for the Customer in respect of each of that Customer's Tenancies. These are also implemented in a multi-tenant manner using shared storage infrastructure.

Within the *Tenant Catalog*, the details of each Customer's *DataStore* (for that Customer's Tenancy in question) are recorded. Each DataStore is implemented as a separate database with its own Credentials that permit access only to that database and not to any other Customer's database or any other database in respect of any other Tenancy.

> *Think of each Customer's DataStore as a book on a shared bookshelf. Ownership of the book is recorded in the Tenant Catalog, and access to open the book requires the credentials that are recorded in the Tenant Catalog. Only Cyferd (as the librarian in this example) has access to the Tenant Catalog.*

Authorized Users can access these *DataStores* only via the *Compute Tier* interfaces. Cyferd staff are not permitted to access the content of the *DataStores* unless authorized by the Customer in question as an Authorized User.

The *DataStores* are stored on volumes that are encrypted using '*Industry common practices within Cloud-hosted Infrastructure*'. Data *at Rest* is encrypted.

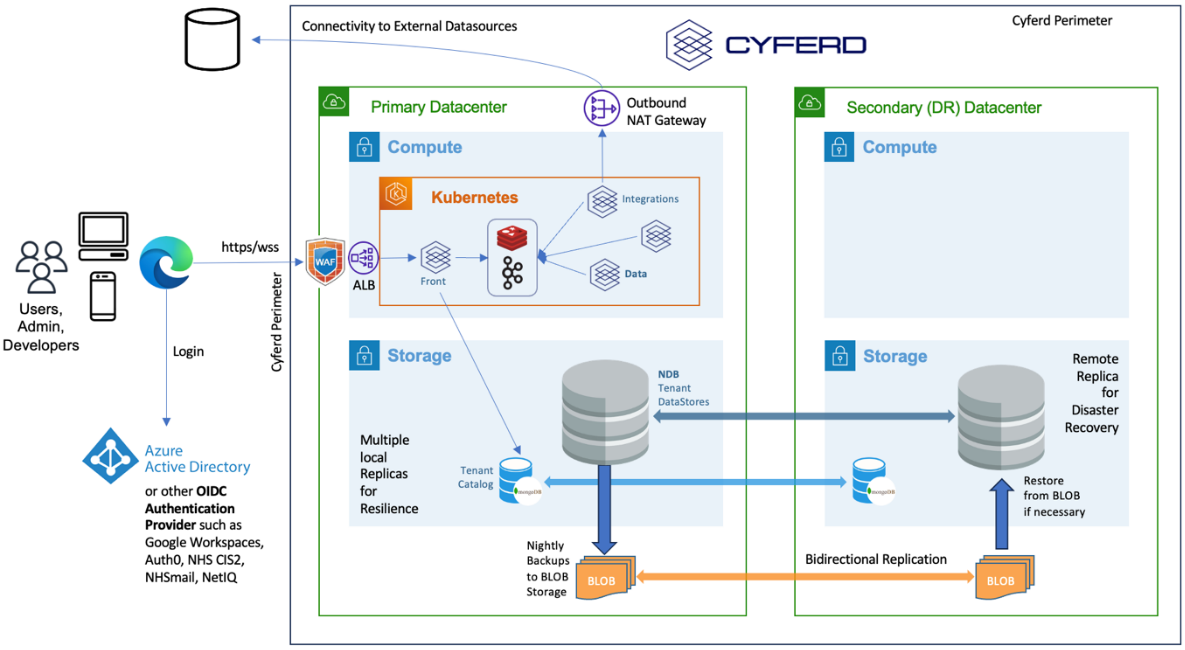
Various technologies are used to manage Customer Data of a Customer (for that Customer's Tenancy(ies) in question). This list describes the main classes of data, but may be modified by Cyferd at any time without notification or obligation:

- **JSON Document**
    - Authorized User *Session* tokens
    - *Transaction Logs* that record *CRUD* operations on managed datasets
    - *Lookup* datasets (values such as Country, Currency, and other categorizations that may be offered in the *User Interface* to be recorded into managed collections of data)
- **Graph & Relational Tables**
    - **Metadata** of objects defined within and used by a Tenancy
        - *Collections* of managed data
        - *Relationships* between *Collections*
        - *Views* that customize the interactions with a *Collection*
        - *Flows* that implement *Business Logic* when interacting with *Collections*
        - *Integrations* – connectivity and authentication details for external datasources that are relevant to the Tenancy in question but not part of the Cyferd Platform
    - **Administrative Data**
        - Properties of Authorized Users who have authenticated into the Tenancy in question or been invited to use it
        - *User Assignments* and *Access Rights*
    - **Cyferd-managed Data**
        - *Collections* (tables)
        - *Relationships* (~ amongst tables)
- **BLOB Storage**
    - *Images* or *Documents* (up to 20MB each) that are uploaded and attached to records in *Collections*
    - Nightly Backups of other *DataStores* within the Tenancy in question

Resilience & Disaster Recovery

Resilience describes the ability to continue service without interruption and may also be known as *High Availability*. When a member of a clustered service must be restarted (e.g. security patches) or replaced (e.g. resized to a larger or newer machine) as part of normal *System Operations* then a resilient configuration provides continuous service without interruption or reconfiguration of clients using that service.

Disaster Recovery (DR) is a process of recovering service to a failover host or environment but is initiated as a consequence of an *interruption of service* due to dramatic failure of connectivity or integrity.


Connectivity to External Datasources
CYFERD
Cyferd Perimeter
Primary Datacenter
Outbound NAT Gateway
Secondary (DR) Datacenter
Compute
Compute
Kubernetes
Integrations
Users, Admin, Developers
https/wss
WAF
ALB
Front
Data
Login
Cyferd Perimeter
Storage
Storage
NDB Tenant DataStores
Remote Replica for Disaster Recovery
Azure Active Directory
or other OIDC Authentication Provider such as Google Workspaces, Auth0, NHS CIS2, NHSmail, NetIQ
Multiple local Replicas for Resilience
Tenant Catalog
Restore from BLOB if necessary
Nightly Backups to BLOB Storage
BLOB
Bidirectional Replication
BLOB

Compute

The *Compute Tier* microservices are implemented in multi-host *Kubernetes clusters* that provide dynamic *Horizontal Pod Autoscaling* based on resource (RAM) utilization. Under heavy utilization, *Kubernetes* will replicate the microservices so that more instances are available to service requests that are on the *Queue*.

A *Kubernetes cluster* can be instantiated in the Secondary Datacenter to leverage local data and restore interrupted customer service in case Cyferd determines or decides that the Primary Datacenter location is inaccessible or compromised.

Storage

To provide *Resilience* against failure of infrastructure *within* the Primary Datacenter location, the *DataStore* technologies have been implemented in *Clusters* that retain two copies of data at the Primary Datacenter location, and a real-time replica in the Secondary Datacenter location in case of any Cyferd decision to initiate a *Disaster Recovery* scenario.

Similarly, the *Image/Document* (*BLOB*) storage is implemented with bidirectional replication between the Primary Datacenter and Secondary Datacenter locations, so that uploaded *Images/Documents* and the nightly Backups are available for restoration from both locations.