

## **Data Access Addendum**

This version applies only to RICOH360 Application and RICOH360 Cloud provided by Ricoh Futures EMEA S.A.S. (“RFE”).

### **1. Definition and Interpretations**

1.1. Under this Data Access Addendum, in addition to the terms defined under the Agreement, the following words have the following meanings.

- (a) “**User**” under a user of RICOH360 Application Terms of Service and RICOH360 Cloud Terms of Service.
- (b) “**Data Holder**” means RFE under RICOH360 Application Terms of Service, RICOH360 Cloud Terms of Service.
- (c) “**Product**” means the following connected product(s): RICOH THETA.
- (d) “**Related Service**” collectively means RICOH360 Application and its related service, RICOH360 Cloud and its related service.
- (e) “**Data**” means any readily available Product Data or Related Service(s) Data within the meaning of the Data Act. Data includes the data listed in **Appendix 1**, with a description of the type or nature, estimated volume, collection frequency, storage location, duration of retention of the Data.
- (f) “**Trade Secret**” means “Trade Secret” within the meaning of Directive (EU) 2016/943.
- (g) “**Trade Secret Holder**” means “Trade Secret Holder” within the meaning of Directive (EU) 2016/943.
- (h) “**Trade Secret Protective Measure**” means the Trade Secret protective measures designated by the Data Holder.
- (i) “**Data Act**” means Regulation (EU) 2023/2854.

1.2. This Data Access Addendum is concluded by the Parties against the background of their rights and obligations under the Data Act. Any provision in this Data Access Addendum must be interpreted to comply with the Data Act, other EU laws, or national legislation adopted in accordance with EU law, as well as any applicable national law that is compatible with EU law and cannot be derogated from by agreement.

### **2. Declaration by the User**

2.1. The User represents and warrants that they are either the owner of the Product or contractually entitled to use the Product under a rent, lease or similar contract and/or to receive the Related Services under a service contract.

2.2. The User must provide upon duly substantiated request to the Data Holder any relevant documentation to support these declarations, where necessary.

### **3. Data use and sharing by the Data Holder**

#### **3.1. Agreed use of non-personal Data by the Data Holder.**

3.1.1. The Data Holder undertakes to use the Data that are non-personal Data only for the purposes agreed with the User as follows:

- (a) Performing an agreement with the User or activities related to such

- agreement.
- (b) Providing support, warranty, guarantee or similar activities or assessing the User's, the Data Holder's or a third party's claims related to Products or Related Services.
  - (c) Monitoring and maintaining the functioning, safety and security of Products or Related Services and ensuring quality control.
  - (d) Maintaining and improving the functioning of, or manufacturing, supplying, or offering any product or (related) service offered by the Data Holder.
  - (e) Developing new products or services by the Data Holder, by third parties acting on behalf of the Data Holder, or in collaboration with other parties.
  - (f) Aggregating these Data with other data or creating derived data, for any lawful purpose, including with the aim of selling or otherwise making available such aggregated or derived data to third parties.
- 3.1.2. The Data Holder undertakes not to use the Data to derive insights about the economic situation, assets and production methods of the User, or about the use of the Product or Related Service by the User in any other manner that could undermine the commercial position of the User on the markets in which the User is active. None of the Data uses agreed to under Clause 3.1 may be in contradiction with this Clause, and the Data Holder undertakes to ensure, by appropriate contractual, organizational and technical means, that no third party, within the Data Holder's organization, engages in such Data use.
- 3.2. Data sharing of non-personal data with third parties**
- 3.2.1. The Data Holder may share with a third party the Data which is non-personal data, if:
- (a) the Data is used by the third party exclusively for the following purposes:
    - (i) Assisting the Data Holder in achieving the purposes permitted under Clause 3.1.1.
    - (ii) Achieving, in collaboration with the Data Holder, the purposes permitted under Clause 3.1.1.
    - (iii) Performing agreements with its customer or activities related to such agreement.
    - (iv) Providing support, warranty, guarantee or similar activities, assessing claims related to the Data by a customer or any other parties, or executing claims related to the Data.
    - (v) Monitoring and maintaining the functioning, safety and security of its products or services and ensuring quality control.
    - (vi) Maintaining and improving the functioning of, or manufacturing, supplying, or offering any product or service offered by the third party.
    - (vii) Developing new products or services by the third party, by any other parties acting on behalf of the third party, or in collaboration with any other parties.
    - (viii) Aggregating these Data with other data or creating derived data, for any lawful purposes, including with the aim of selling or otherwise making available such aggregated or derived data to any other parties.
  - (b) the Data Holder contractually binds the third party:
    - (i) not to use the Data for any purposes or in any way going beyond the

- use that is permissible in accordance with previous Clause 3.2.1 (a);
  - (ii) not to use the Data to derive insights about the economic situation, assets and production methods of the User, or about the use of the Product or Related Service by the User in any other manner that could undermine the commercial position of the User on the markets in which the User is active in accordance with previous Clause 3.2.1 (b); and
  - (iii) to apply the protection measures which is at least in the same level as required under Clause 3.5;
- 3.2.2. Notwithstanding Clause 3.2.1, the Data Holder may use processing services, such as cloud computing services (including infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS)), hosting services, or similar services to achieve, for their own account and under their own responsibility, the agreed purposes under Clause 3.1.1. The third parties may also use such services to achieve, for their own account and under their own responsibility, the agreed purposes under Clause 3.2.1 (a).
- 3.3. **Irrevocable Use and Sharing of Data.**
- 3.3.1. The User hereby grants to the Data Holder an irrevocable license to use and share the Data in accordance with Clauses 3.1 and 3.2.
- 3.4. **Use and Sharing of Personal Data by the Data Holder.**
- 3.4.1. The Data Holder may use, share with third parties or otherwise process any Data that is personal data, only if there is a legal basis provided for and under the conditions permitted under Regulation (EU) 2016/679 (GDPR) and, where relevant, Directive 2002/58/EC (Directive on privacy and electronic communications).
- 3.5. **Protection measures taken by the Data Holder.**
- 3.5.1. The Data Holder undertakes to apply the protection measures to prevent Data loss and unauthorised access to the Data that are reasonable in the circumstances, considering (a) the state of science and technology, (b) potential harm suffered by the User and (c) the costs associated with the protective measures.

#### **4. Data access by the User upon request**

##### **4.1. Obligation to make Data available.**

- 4.1.1. The Data must be made accessible to the User by the Data Holder, at the request of the User or a party acting on their behalf. The request can be made using the form as specified by the Data Holder. For the purpose of verifying that the request is made by the User, the Data Holder shall not require to provide any information beyond what is necessary. If the request is made by a party acting on behalf of the User, evidence of their mandate shall be attached to the request.
- 4.1.2. When the User is not a data subject, the Data Holder shall make the Data which is personal data only available to the User, when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) and only,

where relevant, the conditions set out in Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC (Directive on privacy and electronic communications) are met. In that respect, when the User is not a data subject, the User must indicate to the Data Holder, in each request presented under the previous Clause, the legal basis for processing under Article 6 of Regulation (EU) 2016/679 (and, where relevant, the applicable derogation under Article 9 of that Regulation and Article 5(3) of Directive (EU)2002/58) upon which the making available of personal data is requested.

#### 4.2. **Data characteristics and access arrangements.**

4.2.1. The Data Holder must make the Data available to the User, free of charge for the User, with at least the same quality as it becomes available to the Data Holder, and in any case in a comprehensive, structured, commonly used and machine-readable format. The Data Holder and User may use the services of a third party (including a third-party providing Data Intermediation Services as defined by Article 2 of Regulation (EU) 2022/868) to allow the exercise of the User's rights under Clause 4.1 of this Data Access Addendum. Such third party will not be considered a data recipient under the Data Act ("**Data Recipient**") and such services may be offered by a provider considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925, unless they process the Data for its own business purposes.

4.2.2. The User must receive access to the requested Data (a) easily and securely; and (b) without undue delay.

4.2.3. In order to meet the requirements of Clauses 4.2.1 and 4.2.2, the Data Holder specifies these access arrangements in **Appendix 1**.

4.2.4. The Data Holder must provide to the User, at no additional cost, the information necessary for accessing the Data in accordance with Article 4 of the Data Act. This includes, in particular, the provision of information readily available to the Data Holder regarding any rights which third parties might have with regard to the Data, such as rights of data subjects arising under Regulation (EU) 2016/679 (GDPR), or facts that may give rise to such rights.

4.2.5. The Data Holder must not keep any information on the User's access to the requested Data beyond what is necessary for:

- (a) the sound execution of (i) the User's access request and (ii) this Data Access Addendum;
- (b) the security and maintenance of the data infrastructure; and
- (c) compliance with legal obligations on the Data Holder to keep such information.

#### 4.3. **Feedback loops.**

4.3.1. If the User identifies an incident involving (i) Data covered by this Data Access Addendum, (ii) the requirements of Clauses 4.2.1 or 4.2.2 or (iii) the requirement of Appendix 1 on the Data characteristics and access arrangements, and if the User notifies the Data Holder with a detailed description of the incident, the Data Holder and the User must cooperate in good faith to identify the reason of the incident. If the incident was caused by a failure of the Data Holder to comply with their obligations, they must remedy the breach within a reasonable period of time.

#### 4.4. **Unilateral changes by the Data Holder.**

4.4.1. The Data Holder may unilaterally change the specifications of the Data

characteristics or the access arrangements stated in Appendix 1, if this is objectively justified by the normal conduct of business of the Data Holder, in particular for reasons beyond the control of the Data Holder, for example by a technical modification due to an immediate security vulnerability in the line of the Products or Related Services, a change in the Data Holder's infrastructure made necessary by circumstances outside the influence of the Data Holder or a change in applicable law. For the avoidance of doubt, this Clause does not permit unilateral amendments to the Agreement itself, but solely allows for adjustments to the performance specifications under the existing contractual framework. Any change must meet the requirements of Clauses 4.2.1 and 4.2.2. The Data Holder must give advance notice of the change to the User, with the explanation of the change, before or at least at the same time that the change takes effect.

## **5. Protection of trade secrets**

### **5.1. Applicability of trade secret arrangements.**

5.1.1. Under this Data Access Addendum, the following terms have the following meanings:

- (a) **"Identified Trade Secret"** means Data which is protected as trade secrets (as defined in Article 2(1) of the Trade Secrets Directive (EU) 2016/943), held by the Trade Secrets Holder, and designated as Data protected as trade secrets in **Appendix 2**.
- (b) **"Trade Secret Holder"** means the Data Holder and/or another trade secret holder (as defined in Article 2(2) of said Directive) as identified in **Appendix 2**.

5.1.2. The protective measures set out in Clauses 5.2 and 5.3 of this Data Access Addendum, as well as the related rights agreed in Clauses 5.4, apply exclusively to Identified Trade Secrets.

5.1.3. If, during the term of this Data Access Addendum, new data are made available to the User that is protected as trade secrets, at the request of the Data Holder, **Appendix 2** will be amended accordingly. Until **Appendix 2** has been amended and agreed between the Parties, the Data Holder may temporarily suspend the sharing of the new data protected as trade secrets in accordance with the procedure under the Data Act.

5.1.4. The obligations set out in Clauses 5.2 and 5.3 remain in effect after any termination of this Data Access Addendum, unless otherwise agreed by the parties.

### **5.2. Protective measures taken by the User.**

5.2.1. The User must apply the protective measures set out in **Appendix 2** (the **"User's Protection Measures"**).

5.2.2. If the User is permitted to make Identified Trade Secrets available to a third party, the User must:

- (a) inform the Data Holder without undue delay of the fact that Identified Trade Secrets have been or will be made available to a third party,
- (b) specify the Identified Trade Secret in question, and
- (c) give the Data Holder the identity, place of establishment and contact details of the third party.

5.2.3. The Data Holder may, or may have external auditors, during reasonable business hours and upon reasonable prior notice, audit the User's compliance with Clauses 5.2 of this Data Access Addendum and the User's operational and security policies and procedures, including, but not limited to, the User's physical site security and information security, confidentiality practices and standards with respect to trade secrets.

5.3. **Protective measures taken by the Trade Secret Holder.**

5.3.1. The Data Holder may apply the measures set out in **Appendix 2** and the measures increased or agreed pursuant to Clauses 5.4.1(a) and 5.4.1(b) to preserve the confidentiality of the Identified Trade Secrets ("**Data Holder's Protection Measures**").

5.3.2. The User undertakes not to alter or remove the Data Holder's Protection Measures, unless otherwise agreed by the Parties.

5.4. **Obligation to share and right to refuse, withhold or terminate.**

5.4.1. Where the User's Protection Measures and the Data Holder's Protection Measures do not materially suffice to adequately protect a particular Identified Trade Secret as trade secret, the Data Holder may, by giving notice to the User with a detailed description of the inadequacy of the measures:

(a) unilaterally increase the protection measures regarding the specific Identified Trade Secret in question, provided this increase is compatible with their obligations under this Data Access Addendum and does not negatively affect the User; or

(b) request that additional protection measures be agreed. If there is no agreement on the necessary additional measures after a reasonable period of time and the Data Holder reasonably believes the additional measures are effective to protect the Identified Trade Secret as trade secret, the Data Holder may suspend the sharing of the specific Identified Trade Secret in question. In such case, the Data Holder must give notice to the User. The notice must be duly substantiated, indicate which measures have not been agreed, and be given in writing without undue delay. The Data Holder must continue to share any Identified Trade Secret other than these specific Identified Trade Secret.

5.4.2. If, in exceptional circumstances, the Data Holder is highly likely to suffer serious economic damage from disclosure of a particular Identified Trade Secret to the User despite the User's Protection Measures and the Data Holder's Protection Measures having been implemented, the Data Holder may refuse or suspend sharing the specific Identified Trade Secret in question. The Data Holder must give a duly substantiated notice without undue delay to the User and to the competent authority designated pursuant to Article 37 of the Data Act. However, the Data Holder must continue to share any Identified Trade Secret other than those specific Identified Trade Secret.

5.4.3. If the Data Holder reasonably believes that the User failed or will fail to implement and maintain their User's Protection Measures, the Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secret, until the User has resolved the non-compliance and risk of non-compliance. In this case, the Data Holder must, without undue delay, give duly substantiated notice in writing to the User and to the competent authority designated pursuant to Article 37 of the

Data Act.

5.4.4. Clause 5.4.1 does not entitle the Data Holder to terminate this Data Access Addendum. Clauses 5.4.2 or 5.4.3 entitle the Data Holder to terminate this Data Access Addendum only with regard to the specific Identified Trade Secret if:

- (a) all the conditions of Clause 5.4.2 or Clause 5.4.3 have been met;
- (b) no resolution has been found by Parties after a reasonable period of time, despite an attempt to find an amicable solution, including after intervention by the competent authority designated under Article 37 of the Data Act; and
- (c) the User has not been awarded by a competent court with court decision obliging the Data Holder to make the Identified Trade Secret available and there is no pending court proceedings for such a decision.

#### 5.5. **End of production and destruction of infringing goods.**

5.5.1. Without prejudice to other remedies available to the Data Holder in accordance with this Data Access Addendum or applicable law, if the User alters or removes technical protection measures applied by the Data Holder or does not maintain the technical and organizational measures taken by them in agreement with the Data Holder in accordance with Clauses 5.2 and 5.3, the Data Holder may request the User:

- (a) to erase the data made available by the Data Holder or any copies thereof; and/or
- (b) end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through the Identified Trade Secret, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods; and/or
- (c) compensate a party suffering from the misuse or disclosure of such unlawfully accessed or used data.

#### 5.6. **Retention of Data protected as Identified Trade Secrets.**

5.6.1. Where the Data Holder exercises the right to refuse, withhold or suspend the sharing of Identified Trade Secrets to the User in accordance with Clauses 5.4.1, 5.4.2 and 5.4.3, the Data Holder must ensure that the particular Identified Trade Secret that is the subject matter of the exercising of such right is retained, so that said Identified Trade Secret will be made available to the User:

- (a) once the appropriate protections are agreed and implemented, or
- (b) a binding decision by a competent authority or court is issued requiring the Data Holder to provide the said Identified Trade Secret to the User.

Above retention obligation ends where a competent authority or court in a binding decision allows the deletion of such retained Identified Trade Secret or where this Data Access Addendum terminate.

5.6.2. The Data Holder must bear the necessary costs for retaining the data under Clause 5.6.1. However, the User must cover such costs to the extent the withholding or suspension of Data sharing occurs in accordance with Clause 5.4.3.

## 6. **Data use by the User**

## **6.1. Permissible use and sharing of data.**

6.1.1. The User may use the Data made available by the Data Holder upon their request for any lawful purpose and/or, to the extent that the Data is transferred to or can be retrieved by the User, share the Data freely subject to the limitations in Clause 6.2.

## **6.2. Unauthorised use and sharing of data and restrictions for security reasons.**

6.2.1. The User undertakes not to engage in the following:

- (a) use the Data to develop a connected product that competes with the Products, nor share the Data with a third party for that purpose;
- (b) use such Data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable, the Data Holder;
- (c) use coercive means or abuse gaps in the Data Holder's technical infrastructure which is designed to protect the Data in order to obtain access to Data; or
- (d) share the Data with a third-party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925.

6.2.2. Furthermore and in accordance with Article 4 (2) of the Data Act, the User and the Data Holder agree to restrict or prohibit processing, including accessing, using and/or further sharing of the Data, which could undermine security requirements for the Product, as laid down by applicable EU law and EU member state law, resulting in a serious effect on the health, safety or security of natural persons.

## **7. Data sharing upon the User's request with a Data Recipient**

### **7.1. Making Data available to a Data Recipient.**

7.1.1. The Data must be made available to a Data Recipient by the Data Holder, free of charge for the User, upon request presented by the User or a party acting on its behalf. The request can be made using the form as separately specified by the Data Holder. For the purpose of verifying that the request is made by the User, the Data Holder shall not require to provide any information beyond what is necessary. If the request is made by a party acting on behalf of the User, evidence of their mandate shall be attached to the request. Notwithstanding the foregoing, the Data Holder is not obligated to make available the Data to any third party if it is entitled or required to refrain from doing so under the Data Act or any other applicable laws.

7.1.2. When the User is not a data subject, the Data Holder shall make the Data which is personal data only available to a third party following a request of the User, when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) and only, where relevant, the conditions set out in Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC (Directive on privacy and electronic communications) are met. In that respect, when the User is not a data subject, the User must indicate to the Data Holder, in each request presented under the previous Clause, the legal basis for processing under Article 6 of Regulation (EU) 2016/679 (and, where relevant, the applicable derogation under Article 9 of that Regulation and Article 5(3) of Directive (EU) 2002/58) upon which the making available of personal data is requested.

7.1.3. The Data Holder must make the Data available to the data recipient with at least the

same quality as they become available to the Data Holder, and in any case in a comprehensive, structured, commonly used and machine-readable format, easily and securely.

- 7.1.4. Where the User submits such a request, the Data Holder will agree with the data recipient the arrangements for making the Data available in accordance with Chapter III and Chapter IV of the Data Act.
- 7.1.5. The User acknowledges that a request under Clause 7.1.1 cannot benefit a third party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925 and cannot be made in the context of the testing of new connected products, substances or processes that are not yet placed on the market.
- 7.1.6. The User represents and warrants that the Data Recipient will only process the Data made available to them pursuant to Clause 7.1.1 for the purposes and under the conditions agreed with the User. The Data Holder may not be held liable towards the User for the absence of such an agreement between the User and the data recipient, unless the Data Holder knew or should have known of such absence due to gross negligence.

## **8. Date of application, duration of this Data Access Addendum and termination**

- 8.1. Date of application and duration. This Data Access Addendum shall be effective from the date the User declares assent under Clause 1.1 and continue to apply for the term of the Agreement, subject to any grounds for expiry or termination under this contract.
- 8.2. **Termination.**
  - 8.2.1. Irrespective of the contract period agreed under Clause 9.1, this Data Access Addendum terminate:
    - (a) upon the destruction of the Products or permanent discontinuation of the Related Services, or when the Products or Related Services lose their capacity to generate the Data in an irreversible manner; or
    - (b) upon the User losing ownership of the Products or when the User's rights with regard to the Products under a rental, lease or similar agreement or the User's rights with regard to the Related Services come to an end; or
    - (c) when both Parties so agree.

Points (b) and (c) shall be without prejudice to the contract remaining in force between the Data Holder and any Subsequent or Additional User.

## **8.3. Effects of expiry and termination.**

- 8.3.1. Expiry of the contract period or termination of this Data Access Addendum releases both Parties from their obligation to effect and to receive future performance but does not affect the rights and liabilities that have accrued up to the time of expiry or termination. Expiry or termination does not affect any provision in this Data Access Addendum which is to operate even after this Data Access Addendum have come to an end.
- 8.3.2. The termination or expiry of this Data Access Addendum will have the following effects:

- (a) the Data Holder shall cease to retrieve the Data generated or recorded as of the date of termination or expiry; and
- (b) the Data Holder remains entitled to use and share the Data generated or recorded before the date of termination or expiry as specified in this Data Access Addendum.

## **9. Remedies for breach of this Data Access Addendum**

### **9.1. Cases of non-performance.**

9.1.1. A non-performance of an obligation by a Party is fundamental to this Data Access Addendum if:

- (a) the non-performance substantially deprives the aggrieved Party of what it was entitled to expect under this Data Access Addendum, unless the non-performing Party did not foresee and could not reasonably have foreseen that result; or
- (b) it is clear from the circumstances that the non-performing Party's future performance cannot be relied on.

9.1.2. A Party's non-performance is excused if it is due to an impediment beyond its control and that the non-performing Party could not reasonably have been expected to take the impediment into account at the time of the conclusion of this Data Access Addendum, or to have avoided or overcome the impediment or its consequences. Where the impediment is only temporary the excuse has effect for the period during which the impediment exists. However, if the resulting delay is so significant that it constitutes a fundamental non-performance, the other Party may treat it as such and exercise the remedies available for fundamental non-performance. The non-performing Party must ensure that notice of the impediment and of its effect on its ability to perform is received by the aggrieved Party without undue delay after the non-performing Party knew or could be reasonably expected to have become aware of these circumstances. The aggrieved Party is entitled to damages for economic damage resulting from the non-receipt of such notice.

### **9.2. Remedies.**

9.2.1. Clauses related to the remedies for breach under the Agreement shall be applied mutatis mutandis to this Data Access Addendum. Additionally, and without prejudice to any remedies available under applicable law, in the case of a non-performance by a Party under this Data Access Addendum, the aggrieved Party will have the remedies listed in the following Clauses:

9.2.2. Remedies which are not incompatible may be cumulated.

9.2.3. The aggrieved Party may not resort to a remedy to the extent that they cause the other Party's non-performance, such as where a shortcoming in its own data infrastructure did not allow the non-performing Party to duly perform its obligations. The aggrieved Party may also not rely on a claim for damages suffered to the extent that it could have reduced the damage by taking reasonable steps.

9.2.4. The aggrieved Party can:

- (a) request that the non-performing Party comply, without undue delay, with its obligations under this Data Access Addendum, unless it would be unlawful or impossible or unless such specific performance would cause the non-performing Party costs which are disproportionate to the benefit the

- aggrieved Party would obtain;
  - (b) request that the non-performing Party erases Data accessed or used in violation of this Data Access Addendum and any copies thereof;
  - (c) claim damages for economic damage caused to them by the other Party's non-performance which is not excused under Clause 10.1.2. Any legal obligation under applicable law to first issue a formal reminder to the non-performing Party or to set a deadline for performance or subsequent performance remain unaffected. The non-performing Party is liable only for damage which it foresaw or could be reasonably expected to have foreseen at the time of conclusion of this Data Access Addendum as a result of its non-performance, unless the non-performance was intentional or grossly negligent.
- 9.2.5. The Data Holder can also suspend the sharing of Data with the User until the User complies with their obligations, by giving a duly substantiated notice to the User without undue delay:
- (a) if the non-performance of User's obligations is fundamental; or
  - (b) provided that all other conditions set out in Clause 5.4.3 are met, in cases described in Clause 5.4.3.

**10. Order of precedence**

- 10.1. In the event of any conflict or inconsistency between these clauses on this Data Access Addendum and any other applicable contractual arrangements, terms, conditions or other applicable agreements related to this Data Access Addendum these clauses will take precedence.