EU DATA ACT TERMS

These EU Data Act Terms (these "EU Terms") are incorporated into and made part of that certain Fiery End User License Agreement (the "EULA") You agreed to when accessing Fiery software and/or products. Capitalized terms not defined herein shall have the same meaning as ascribed to them in the EULA.

1. Parties and Product/Related Service

"Data Holder" shall refer to Fiery, LLC and its subsidiaries and affiliates. "User" shall refer to You. Data Holder and User are referred to below collectively as 'the Parties' and individually as 'the Party'.

1.1 Product/Related Service

These EU Terms are made with regard to:

(a) the following connected product(s) (the 'Product') and related services ("Related Services"): The Fiery Software for which the Fiery End User License Agreement applies;

The User declares 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 Service(s) under a service contract.

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

2. Data covered by these EU Terms

The data covered by these EU Terms (the 'Data') consist of any readily available Product Data or Related Service(s) Data within the meaning of the Data Act.

The Data consist of the Data listed in **Appendix 1**, with a description of the type or nature, estimated volume, collection frequency, storage location and duration of retention of the Data.

If, during these EU Terms, new data are made available to the User, **Appendix 1** will be amended accordingly.

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 any agreement with the User or activities related to such agreement (e.g. issuing invoices, generating and providing reports or analysis, financial projections, impact assessments, calculating staff benefit);

(b) providing support, warranty, guarantee or similar services or to assess User's, Data Holder's or third party's claims (e.g. regarding malfunctions of the Product) related to the Product or Related Service;

(c) monitoring and maintaining the functioning, safety and security of the Product or Related Service and ensuring quality control;

(d) improving the functioning of any product or related service offered by the Data Holder;

(e) developing new products or services, including artificial intelligence (AI) solutions, by the Data Holder, by third parties acting on behalf of the Data Holder (i.e. where the Data Holder decides which tasks will be entrusted to such parties and benefits therefrom), in collaboration with other parties or through special purpose companies (such as joint ventures);

(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, provided such data do not allow specific data transmitted to the Data Holder from the connected product to be identified or allow a third party to derive those data from the dataset.

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 3.1.1 may be interpreted as including such Data use, and the Data Holder undertakes to ensure, by appropriate organisational and technical means, that no third party, within or outside the Data Holder's organisation, engages in such Data use.

3.2 Sharing of non-personal data with third parties and use of processing services

3.2.1 The Data Holder may share with third parties the Data and 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 or through special purpose companies, the purposes permitted under clause 3.1.1;

iii) purposes for which the User consents or authorizes such third party to use its Data (such as for services, assistance, or otherwise that the User has requested from such third party);

(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) to comply with clause 3.1.2;

iii) to apply the protective measures required under clause 3.4.1; and

iv) not to share these Data further unless the User grants general or specific agreement for such further transfer, or unless such Data sharing is required, in the interest of the User, to fulfil these EU Terms or any contract between the third party and the User If the User agrees to the further transfer, the Data Holder should oblige the third party with whom they share Data to include the clauses corresponding to points (i) to (iv) in their contracts with recipients.

3.2.2 The Data Holder may always use processing services, e.g. cloud computing services (including infrastructure as a service, platform as a service and software as a service), hosting services, or similar services to achieve the agreed purposes under clause 3.1. The third parties may also use such services to achieve the agreed purposes under clause 3.2.1 (a).

3.3 Use and Sharing of Personal Data by the Data Holder

The Data Holder may use, share with third parties or otherwise process any Data that is personal data, under 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).

3.4 Protection measures taken by the Data Holder

3.4.1 The Data Holder undertakes to apply the protective measures for the Data that are reasonable in the circumstances, considering the state of science and technology, potential harm suffered by the User as a result of Data loss or disclosure of Data to unauthorised third parties and the costs associated with the protective measures.

3.4.2 The Data Holder may also apply other appropriate technical protection measures to prevent unauthorised access to Data and to ensure compliance with these EU Terms.

3.4.3 The User agrees not to alter or remove such technical protection measures.

4. Data access by the User upon request

4.1 Obligation to make data available

4.1.1 The Data, together with the relevant metadata necessary to interpret and use those 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 at https://www.fiery.com/EU_Data_Act.

4.1.2 The Data Holder shall make the Data which is personal data available to the User, when the User is not the data subject, only 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 the 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 as well as the relevant metadata necessary to interpret and use those Data.

The Data Holder must specify the Data characteristics and inform the User of these specifications in **Appendix 1**.

4.2.2 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 these EU Terms. Such third party will not be considered a Data Recipient under the Data Act, unless they process the Data for its own business purposes. The party requiring the use of such a third party must notify the other party in advance.

4.2.3 The User must receive access to the Data: easily and securely by the Data being transmitted or by access to the Data where it is stored;

and

The Data Holder must specify these access arrangements and inform the User of these specifications in **Appendix 1**.

4.2.4 The Data Holder must provide to the User, at no additional cost, the means and information strictly 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 the origin of the Data and 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.

In order to meet these requirements, the Parties agree on the specifications set out in **Appendix 1**, which forms an integral part of these EU Terms.

4.3 Feedback loops

If the User identifies an incident related to clause 2 on the Data covered by these EU Terms, to the requirements of clauses 4.2.1 or 4.2.3 or of **Appendix 1** on the Data quality 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. If the Data Holder does not do so, it is considered as a fundamental breach and the User may invoke clause 12 of these EU Terms (remedies for non-performance). If the User considers their access right under Article 4 (1) of the Data Act to be infringed, the User is also entitled to lodge a complaint with the competent authority, designated in accordance with Article 37(5), point (b) of the Data Act.

4.4 Unilateral changes by the Data Holder

The Data Holder may, in good faith, unilaterally change the specifications of the Data or the access arrangements stated in **Appendix 1**, if this is objectively justified by the general conduct of business 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 or a change in the Data Holder's infrastructure.

The Data Holder must in this case give notice of the change to the User without undue delay after deciding on the change. Where the change may negatively affect Data access and use by the User more than just to a small extent, the Data Holder must give notice to the User at least ten days' notice before the change takes effect.

A shorter notice period may only suffice where such notice would be impossible or unreasonable in the circumstances, such as where immediate changes are required because of a security vulnerability that has just been detected.

4.5 Information on the User's access

The Data Holder undertakes not to 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) these EU Terms;

(b) the security and maintenance of the data infrastructure; and

(c) compliance with legal obligations on the Data Holder to keep such information.

5. Applicability of trade secret arrangements

5.1.1 The protective measures agreed on in clauses 5.2. and 5.3 of these EU Terms, as well as the related rights agreed in clauses 5.4, apply exclusively to Data or metadata included in the Data to be made available by the Data Holder to the User, which are protected as trade secrets (as defined

in the Trade Secrets Directive (EU) 2016/943), held by the Data Holder or another Trade Secret Holder (as defined in said Directive).

5.1.2 Data Holder does not believe trade secrets are part of the Data and will not disclose any trade secrets to User.

5.1.3 If, during these EU Terms, new data are made available to the User that is protected as trade secrets as set forth in clause 5.1.1, Data Holder will provide an appendix of such trade secrets.

Until the Trade Secret Appendix has been amended and agreed between the Parties, the Data Holder may temporarily suspend the sharing of the specific newly Identified Trade Secret(s) by

giving notice to the User and the competent authority designated under Article 37 of the Data Act, with a copy of this sent to the User.

5.1.4 The obligations set out in clauses 5.2 and 5.3 remain in effect after any termination of these EU Terms, 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 by Data Holder to the extent any trade secrets are identified in the Data ("Identified Trade Secrets U Measures").

5.2.2 If the User is permitted to make Data protected as Trade secrets available to a third party, the User must inform the Data Holder of the fact that Identified Trade Secrets have been or will be made available to a third party, specify the Data in question, and give the Data Holder the identity and contact details of the third party.

5.2.3 In order to verify if and to what extent the User has implemented and is maintaining the Identified Trade Secrets EU Measures, the User agrees to either (i) annually obtain, at User's expense, a security conformity assessment audit report from an independent third party chosen by the User, or (ii) to annually allow, at Data Holder's expense, a security conformity assessment audit from an independent third party chosen by the Data Holder, subject to such independent third party having signed a confidentiality agreement as provided by the User. Such security audit report must demonstrate User's compliance with availability, integrity, confidentiality principles as further described in the Trade Secrets Appendix as applicable at that time. The results of the audit reports will be submitted to both Parties without undue delay.

The User may choose between (i) and (ii). If the User opts for a security audit from an independent third party at Data Holder's expense as set forth above, it retains the right to obtain security audit report from an independent third party at User's expense if it deems the security audit report from an independent third party at Data Holder's expense is not correct. If this right is exercised, both independent third-party auditors, together with Parties, will discuss any difference between those two reports and aim to resolve any pending materials matters while observing good faith.

5.3 Protective measures taken by the Data Holder

5.3.1 The Data Holder may apply any appropriate technical and organisational protection measures to preserve the confidentiality of the shared and otherwise disclosed Identified Trade Secrets (hereinafter: 'Identified Trade Secrets DH Measures').

5.3.2 The Data Holder may also add unilaterally appropriate technical and organisational protection measures, if they do not negatively affect the access and use of the Data by the User under these EU Terms.

5.3.3 The User undertakes not to alter or remove such Identified Trade Secrets DH Measures, unless otherwise agreed by the Parties.

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

5.4.1 The Data Holder must share the Data, including Identified Trade Secrets, in accordance with

these EU Terms, and may not refuse, withhold or terminate the sharing of any Identified Trade Secrets, except as explicitly set forth in the clauses 5.4.2, 5.4.3 and 5.4.4.

5.4.2 Where the Identified Trade Secrets U Measures and the Identified Trade Secrets DH Measures do not materially suffice to adequately protect a particular Identified 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 its obligations under these EU Terms 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 if the need of such measures is duly substantiated, e.g. in a security audit report, the Data Holder may suspend the sharing of the specific Identified Trade Secret by giving notice to the User and to the competent authority designated pursuant to Article 37 of the Data Act, with copy of this sent to the User.

The Data Holder must continue to share any Identified Trade Secrets other than these specific Identified Trade Secrets.

5.4.3 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 Identified Trade Secrets U Measures and the Identified Trade Secrets DH Measures having been implemented, the Data Holder may stop sharing the specific Identified Trade Secret in question.

They may do this only if they give a duly substantiated notice to the User and to the competent authority designated pursuant to Article 37 of the Data Act, with a copy being sent to the User.

However, the Data Holder must continue to share any Identified Trade Secrets other than those specific Identified Trade Secrets.

5.4.4 If the User fails to implement and maintain their Identified Trade Secrets U Measures and if this failure is duly substantiated by the Data Holder, e.g. in a security audit report from an independent third party, the Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secrets, until the User has resolved the incident or other issue as described in the following two paragraphs.

In this case, the Data Holder must, without undue delay, give duly substantiated notice to the User and to the competent authority designated pursuant to Article 37 of the Data Act, with a copy sent to the User.

On receiving this notice, the User must address the incident/issue without undue delay (i.e., they must (i) assign the appropriate priority level to the incident/issue based on its potential detrimental impact and (ii) resolve the issue in consultation with the Data Holder and otherwise in accordance with the applicable proceedings as set out in Trade Secrets Appendix).

5.4.5 Clause 5.4.2 does not entitle the Data Holder to terminate these EU Terms.

Clauses 5.4.3 or 5.4.4 entitle the Data Holder to terminate these EU Terms only with regard to the specific Identified Trade Secrets, and if:

(i) all the conditions of clause 5.4.3 or clause 5.4.4 have been met;

(ii) no resolution has been found by Parties after *(insert 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

(iii) the User has not been awarded by a competent court with court decision obliging the Data Holder to make the Data available and there is no pending court proceedings for such a decision.

5.5 End of production and destruction of infringing goods

Without prejudice to other remedies available to the Data Holder in accordance with these EU Terms or applicable law, if the User alters or removes technical protection measures applied by the Data Holder or does not maintain the technical and organisational 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 Secrets, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those data will cause significant harm to the Data Holder or the Trade Secret Holder or where such a measure would not be disproportionate in light of the interests of the Data Holder or the Trade Secret Holder; 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 under clauses 5.4.2, 5.4.3 and 5.4.4 the Data Holder exercises the right to withhold, suspend or in any other way end or refuse the data sharing to the User, it will need to ensure that the particular Data that is the subject matter of the exercising of such right is retained, so that said Data 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 Data to the User.

Above retention obligation ends where a competent authority or court in a binding decision allows the deletion of such retained data or where these EU Terms terminates.

5.6.2 The Data Holder will bear the necessary costs for retaining the data under clause 5.6.1. However, the User will cover such costs in part or in full where and to the extent the withholding, suspension or refusal to provide data was caused by the User acting in bad faith**.**

6. Data use by the User

6.1 Permissible use and sharing of data

The User may use the Data made available by the Data Holder upon their request for any lawful purpose and/or share the Data freely subject to the limitations below.

6.2 Unauthorised use and sharing of data

6.1.1 The User undertakes not to engage in the following:

(a) use the Data to develop a connected product that competes with the Product, nor share the Data with a third party with that intent;

(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 to obtain access to Data or, for that purpose, abuse gaps in the Data Holder's technical infrastructure which is designed to protect the Data;

(d) share the Data with a third-party considered as a gatekeeper under article 3 of Regulation (EU) 2022/1925;

(e) use the Data they receive for any purposes that infringe EU law or applicable national law.

6.1.2 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 health, safety, or security of natural persons.

6.1.3 been duly notified of any of these restrictions, that result in a refusal to share the Data.]

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, together with the relevant metadata necessary to interpret and use those 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 at https://www.fiery.com/EU_Data_Act/

Users can access the Job log via Command WorkStation (CWS), Fiery IQ, or programmatically via Fiery API.

For Job Metadata, users may submit a request on: https://www.fiery.com/EU_Data_Act/

7.1.2 The Data Holder shall make the Data which is personal data available to a third party following a request of the User, when the User is not the data subject, only 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 the 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 a 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 under fair, reasonable and non-discriminatory terms and in a transparent manner 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 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 Applicable law

These EU Terms are governed by the law of the state of California, USA or a member state where Data Holder elects.

8 Intentionally Omitted

9 Transfer of use and multiple users

9.1 Transfer of use

9.1.1 Where the User contractually transfers (i) ownership of the Product, or (ii) their temporary rights to use the Product, and/or (ii) their rights to receive Related Services to a subsequent natural or legal person ('Subsequent User') and loses the status of a user after the transfer to a Subsequent User, the Parties undertake to comply with the requirements set out in this clause.

9.1.2 The User must:

(a) ensure that the Subsequent User cannot use the initial User's account,

(b) notify the Data Holder of the transfer.

9.1.3 The rights of the Data Holder to use Product Data or Related Services Data generated prior to the transfer will not be affected by a transfer i.e. the rights and obligations relating to the Data transferred under these EU Terms before the transfer will continue after the transfer.

9.2 Multiple users

9.2.1 Where the Initial User grants a right to use of the Product and/or Related Service(s) to another party ('Additional User') while retaining their quality as a user, the Parties undertake to comply with the requirements set out in this clause.

9.2.2 The User must:

ensure that the Additional User cannot use the Initial User's account.

9.3 Liability of the Initial User

If the User's failure to comply with their obligations under clauses 10.1 or 10.2 leads to the use and sharing of Product or Related Services Data by the Data Holder in the absence of a contract with the Subsequent or Additional User, the User will indemnify the Data Holder and hold them harmless in respect of any claims by the Subsequent or Additional User towards the Data Holder for the use of the Data after the transfer.

10 Date of application and duration of these EU Terms and Termination

10.1 Date of application and duration

10.1.1 These EU Terms take immediate effect.

10.1.2 These EU Terms are concluded for unspecified time, unless it expires or is terminated in accordance with clauses 11.2 and 12.2, or the User no longer has the right or ability to use the Product.

10.2 Termination

Irrespective of period agreed under clause 11.1, these EU Terms terminate:

(a) upon the destruction of the Product or permanent discontinuation of the Related Service, or when the Product or Related Service is otherwise put out of service or loses its capacity to generate the Data in an irreversible manner; or

(b) upon the User losing ownership of the Product or when the User's rights with regard to the Product under a rental, lease or similar agreement or the user's rights with regard to the related service come to an end; or

(c) when both Parties so agree, with or without replacing these EU Terms by a new contract.

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

10.3 Effects of expiry and termination

10.3.1 Expiry of these EU Terms period or termination of these EU Terms 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 termination.

Expiry or termination does not affect any provision in these EU Terms which is to operate even after these EU Terms have come to an end, in particular clause 13.1 on confidentiality, clause 13.3 on applicable law and clause 13.6 on dispute resolution, which remain in full force and effect.

10.3.2 The termination or expiry of these EU Terms will have the following effects:

(a) the Data Holder shall immediately cease to retrieve the Data generated or recorded as of the date of termination or expiry;

(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 these EU Terms.

11 Remedies for breach of contract

11.1 Cases of non-performance

11.1.1 A non-performance of an obligation by a Party is fundamental to these EU Terms if:

(a) strict compliance with the obligation is of the essence of these EU Terms, in particular because non-compliance would cause significant harm to the other Party, the User or other protected third parties; or

(b) the non-performance substantially deprives the aggrieved Party of what it was entitled to expect under these EU Terms, unless the other Party did not foresee and could not reasonably have foreseen that result; or

(c) the non-performance is intentional.

11.1.2 A Party's non-performance is excused if it proves that it is due to an impediment beyond its control and that it could not reasonably have been expected to take the impediment into account at the time of the conclusion of these EU Terms, 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 delay amounts to a fundamental non-performance, the other Party may treat it as such.

The non-performing Party must ensure that notice of the impediment and of its effect on its ability to perform is received by the other Party within a reasonable time after the non-performing Party knew or ought to have known of these circumstances. The other Party is entitled to damages for any loss resulting from the non-receipt of such notice.

11.2 Remedies

11.2.1 In the case of a non-performance by a Party, the aggrieved Party shall have the remedies listed in the following clauses, without prejudice to any other remedies available under applicable law.

11.2.2 Remedies which are not incompatible may be cumulated.

11.2.3 A Party may not resort to any of the remedies to the extent that its own act or state of affairs caused the other Party's non-performance, such as where a shortcoming in its own data infrastructure did not allow the other Party to duly perform its obligations. A Party may also not rely on a claim for damages for loss suffered to the extent that it could have reduced the loss by taking reasonable steps.

11.2.4 Each party can:

(a) request that the non-performing Party comply, without undue delay, with its obligations under these EU Terms, unless it would be unlawful or impossible or specific performance would cause the non-performing Party unreasonable effort or expense;

(b) request that the non-performing Party erases Data accessed or used in violation of these EU Terms and any copies thereof;

(c) claim damages for pecuniary damages caused to the aggrieved Party by the non-performance which is not excused under clause 12.1.2. The non-performing Party is liable only for damages which it foresaw or could reasonably have foreseen at the time of conclusion of these EU Terms as a likely result of its non-performance, unless the non- performance was intentional or grossly negligent.

11.2.5 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:

(i) if the non-performance of User's obligations is fundamental;

(ii) provided that, where applicable, all other conditions set out in clause 5.4.3 are met.

11.2.6 The User can also:

(a) suspend the permission given to the Data Holder under clauses 3 or the limitations made under clause 8, until the Data Holder complies with their obligations, unless this would foreseeably cause a detriment to the Data Holder that is obviously disproportionate in the light of the seriousness of the non-performance;

(b) withdraw the permission given to the Data Holder under clauses 3 and/or their agreement to the limitations on User's rights agreed in clause 8, by giving notice to the Data Holder, if:

(i) the Data Holder's non-performance is fundamental; or

(ii) in the case of non-performance which is not fundamental, the user has given a notice fixing a reasonable period of time to remedy the breach and the period has lapsed without the Data Holder remedying the breach. If the period stated is too short, the User may nevertheless terminate these EU Terms, but only after a reasonable period from the time of the notice.

12 General Provision

12.1 Confidentiality

12.1.1 The following information will be considered confidential information:

(a) information referring to the trade secrets, financial situation or any other aspect of the operations of the other party, unless the other Party has made this information public;

(b) information referring to the User and any other protected third party, unless they have already made this information public;

(c) information referring to the performance of these EU Terms and any disputes or other irregularities arising in the course of its performance;

(d) the existence of these EU Terms and the identity of the Parties;

(e) the terms and conditions of these EU Terms.

12.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 13.1.1. and not to disclose or make such information available to any third party unless one of the Parties

(a) is under a legal obligation to disclose or make available the relevant information; or

(b) has to disclose or make the relevant information available in order to fulfil its obligations under these EU Terms, and the other Party or the third party providing the confidential information or affected by its disclosure can reasonably be considered to have accepted this; or

(c) has obtained the prior written consent of the other Party or the party providing the confidential information or affected by its disclosure.

12.1.3 These confidentiality obligations remain applicable after the termination of these EU Terms for a period of (specify the period).

12.1.4 These confidentiality obligations do not remove any more stringent obligations under (i) the Regulation (EU) 2016/679 (GDPR), (ii) the provisions implementing Directive 2002/58/EC or Directive (EU) 2016/943, or (iii) any other Union or Member State law (iv) (if applicable) clause 6 of these EU Terms.

12.2 Means of communication

Any notification or other communication required by these EU Terms must be in writing and may be delivered by hand, sent by prepaid post, or transmitted by electronic means, including email, provided that the sender retains proof of sending to the addresses listed below:

EUDataActSupport@fiery.com

Any such notice or communication will be deemed to have been received:

(a) if delivered by hand, on the date of delivery;
(b) if sent by prepaid post, on the third business day after posting;
(c) if sent by electronic means, on the date of transmission, provided that no error message indicating failure to deliver has been received by the sender.

12.3 Entire Contract, modifications and severability

12.3.1 These EU Terms (together with its appendices and any other documents referred to in these EU Terms) constitutes the entire Contract between the Parties with respect to the subject matter of these EU Terms and supersedes all prior contracts or agreements and understandings of the Parties, oral and written, with respect to the subject matter of these EU Terms.

12.3.2 Any modification of these EU Terms shall be valid only if agreed to in writing, including in any electronic form that, in line with good commercial practices, is considered as fulfilling the requirements of a written document.

12.3.3 If any provision of these EU Terms are found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of these EU Terms, these remaining provisions shall be unaffected by this and will continue to be valid and

enforceable. Any resulting gaps or ambiguities in these EU Terms shall be dealt with according to clause 13.5**.**

12.4 Interpretation

12.4.1 These EU Terms are concluded by the Parties against the background of the Parties' rights and obligations under the Data Act. Any provision in these EU Terms must be interpreted so as to comply with the Data Act and other EU law 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.

12.4.2 If any gap or ambiguity in these EU Terms cannot be resolved in the way referred to by clause 13.5.1, these EU Terms shall be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 13.3) and, in any case, according to the principle of good faith and fair dealing.

12.5 Dispute settlement

12.5.1 The Parties agree to use their best efforts to resolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to (insert name and contact details of a particular dispute settlement body; for disputes within their competences as defined in Article 10 (1) of the Data Act, it may be any dispute settlement body in a Member State that fulfils the conditions of Article 10 of the Data Act elected by Data Holder at the time of dispute).

12.5.2 Submission of a dispute to a dispute settlement body in accordance with clause 13.6.1. does, however, not affect the user's right to lodge a complaint with the national competent authority designated in accordance with Article 37 of the Data Act, or the right of any Party to seek an effective remedy before a court or tribunal in a Member State.

12.5.3 For any dispute that cannot be settled in accordance with clause 13.6.1, the courts of California, USA will, to the extent legally possible, have exclusive jurisdiction to hear the case.

Appendix 1: Details of the data covered by these EU Terms and of access arrangements

1. Specification of data points

Data Type	Job Log Attributes	How It's Captured	Format(s) / Access
Job log	– Device/Group – User – Submitted By – Authorized User – Job Title – Size – Server – Date/Time – Page Description Language – RIP Error – Number Of Copies Of Job Printed – Number Of Pages Printed – Number of Rips Used – Total Number Of Color Pages Printed – Total Number Of Black And White Pages Printed – Print Status – Instructions – Interpreter – Notes – Virtual Printer – Timestamp Spooling – Timestamp Done Spooling – Timestamp Waiting To RIP – Timestamp RIPping – Timestamp Done RIPping – Process Time – Timestamp Waiting To Print – Timestamp Printing – Timestamp Done Printing – Paper Source – Media Type – Media Weight – Paper Catalog Descriptive Name – Paper Catalog Product ID – PCMID Paper Catalog internal Media ID – Output color profile	Generated upon job submission	CSV/Tab-delimited. Data can be accessed via Command WorkStation (CWS), Fiery IQ, or programmatically via Fiery API
Job Metadata	– Job log information – Job submission mode – Color measurement data – Printer and server model – Server configuration and status – Configuration and operational status information from the IoT device.	- Job Metadata is gathered from an agent installed. - The Cloud-hosted application (AWS)	JSON. Submit request on http://www.fiery.com/EU_Data_Act

		gathers and displays metrics. - Data doesn't contain PII or sensitive user/customer data.	

2. Duration of retention

The Fiery Job log is retained indefinitely as long as sufficient storage space remains available on the Fiery server's storage drive.

Job Metadata is retained in Fiery's Cloud-hosted application for 6 months.

3. Data classification

Job Log Data

- **Description:** Records of individual print jobs, which may include details such as job name, user ID, timestamps, and device identifiers.
- **Classification:** *May contain personal data* (e.g., usernames or identifiers that can be linked to an individual).
- **Applicable Regime:** Subject to the **General Data Protection Regulation (GDPR)** and related EU/national data protection laws.
- **Handling:** Access provided under the EU Data Act will be consistent with GDPR requirements, ensuring appropriate safeguards for personal data.

Job Metadata

- **Description:** Non-personal information about job processing, such as job size, color/mono classification, number of pages, and processing time.
- **Classification:** *Non-personal data*.
- **Applicable Regime:** Covered solely by the **EU Data Act**. GDPR does not apply.
- **Handling:** Provided to users in machine-readable formats (JSON) without restriction.

4. Data structure and format

- **Job log:** CSV/Tab-delimited
- **Job Metadata:** JSON

5. Access policy

When the rights to use a Fiery Product or Related Service are transferred to a **Subsequent User** (e.g., resale of a printer with an embedded Fiery DFE, or transfer of license rights) or when **multiple users share the same rights**, the following rules apply:

a. User's Removable Data

- Definition: Data that the original User can delete at their discretion before transfer.

- Fiery Example: User-specific job logs, authentication credentials, stored print jobs, saved workflows, or personal preferences.

- Policy: The User is responsible for deleting this data prior to transfer. If not deleted, such data may become accessible to the Subsequent User.

b. Always Removable Data

- Definition: Data that must never be made accessible to Subsequent Users.

- Fiery Example: Licensing and activation keys tied to the original User, administrative credentials, or cloud service tokens (e.g., Fiery IQ account bindings).

- Policy: The Data Holder (Fiery) will not grant access to this data to Subsequent Users. This data should always be reset or removed during transfer.

c. Residual Data

- Definition: Data that is not removable by the User or not classified as Always Removable. This data may remain on the product or service and be accessible to Subsequent Users by law or in practice.

- Fiery Example: System error codes, generic telemetry, cumulative counters, or data required to ensure product functionality and traceability.

- Policy: Residual Data will remain available to Subsequent Users. Such data is not subject to confidentiality obligations of the original User, since it forms part of the product's operational history.

6. Transfer/Access Medium

Users can access the Job log via Command WorkStation (CWS), Fiery IQ, or programmatically via Fiery API.

For Job Metadata, users may submit a request on: https://www.fiery.com/EU_Data_Act/

7. Means and information necessary for the exercise of the User's access rights

To enable Users to exercise their access rights under the EU Data Act, the following means and information will be provided:

Access Process
Users may submit data access requests through the dedicated portal: **http://www.fiery.com/EU_Data_Act/**. The request form will require User identification, product information (e.g., serial number, product type), and the specific type of data requested. Fiery will confirm receipt and provide a response within **five (5) working days**.

Format of Data
Data will be provided in structured, commonly used, machine-readable formats such as **CSV and JSON**. Where applicable, Fiery will also provide instructions on how to access logs directly from the product.

Technical Support
Users can contact EUDataActSupport@fiery.com for technical questions or issues relating to data access

Data Holder Contact: EUDataActSupport@fiery.com
Fiery OEM partners may designate a corresponding **User-side contact** to coordinate requests from their customer base.

Information Provided to Users
Fiery Servers Product Data Information Disclosure Policy is available on Fiery.com