

General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool

General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool

of WifOR GmbH, Rheinstraße 22, 64283 Darmstadt, Germany

WifOR GmbH, Rheinstraße 22, 64283 Darmstadt, Germany (hereinafter referred to as **“WifOR”**) is currently working on an online tool (the **“WifOR Impact Valuation Tool”**) for access to and usage of data collected and owned or licensed by WifOR (the **“WifOR data”**).

The WifOR Impact Valuation Tool is under steady development, optimization and other changes of its content, design, functions, scope, and technical background. WifOR provides access to the current state of the WifOR Impact Valuation Tool (the **“Beta Version”**) for special users (**“Customers”**).

WifOR and Customer (hereinafter each also referred to as **“Party”** and together the **“Parties”**) therefore agree as follows:

1. Subject, Scope of application

1.1 These General Terms and Conditions specify the terms applicable to the Customer’s access to the Beta Version of the WifOR Impact Valuation Tool. All offers of WifOR and the provision of the Beta Version are made exclusively on the basis of these General Terms and Conditions. Any deviating, conflicting or supplementary general terms and conditions of the Customer are expressly excluded.

1.2 WifOR grants Customer the possibility to access and use the free Beta Version as a software-as-a-service solution via the internet under the provision of this General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool after self-registration of the Customer. WifOR reserves the right to refuse the Customer’s request for access to the free Beta Version and to offer access against payment of license fees based on an individual offer instead. In this case, the offer includes information on the numbers of users, the fees as well as further services (the **“Offer”**, this General Terms and Conditions and the Offer, if any, together referred to as the **“Agreement”**).

- 1.3** In the Beta Version, Customer has the opportunity to use the current state of the functions of the WifOR Impact Valuation Tool. Customer can exploit its own data by using the WifOR data within the WifOR Impact Valuation Tool and by creating own evaluations. For this intend, Customer may upload its own data to the Beta Version and store it for further research.
- 1.4** Customer may have the possibility to choose between different types of WifOR data when using the WifOR Impact Valuation Tool for impact calculation purposes. WifOR will inform the Customer in a reasonable manner if WifOR data is provided by third parties under a public license. In the Beta Version, the Customer may select the publicly available Exiobase 3 dataset for its research. Further information on Exiobase 3 and a hyperlink to the terms and conditions of the public license under which the licensor of the Exiobase 3 datasets grants a right of use are attached as **Annex 1**.

2. Beta Version

- 2.1** The Beta Version is provided on an “as is” basis. Customer is aware that the Beta Version is not supposed to be a full version with full access and full performance. The Beta Version is provided without documentation and without a user manual. Defects, disturbances, and loss of data are possible and cannot be excluded. Therefore, it is the obligation of Customer to review the results generated by use of the Beta Version carefully and to refrain from further use and to notify WifOR immediately if there is any doubt about correctness.
- 2.2** WifOR cannot guarantee that the Beta Version and its server platform are error-free, nor that they can be used without interruption. In particular, WifOR is entitled to suspend access for maintenance work and further development at any time but will notify Customer in good time advance if feasible.
- 2.3** WifOR reserves the right to restrict Customer’s use of the Beta Version in the event of excessive use by Customer that leads to a system or network load on WifOR’s server capacities. WifOR shall notify Customer of any such overload and shall jointly endeavor with Customer to take appropriate remedial action.

3. Access Rights

- 3.1** The software provided in the Beta Version is not physically transferred to Customer.

3.2 Customers may request access to the free Beta Version by entering their e-mail address in the online form and following the registration process. It is at the sole discretion of WifOR whether WifOR offers the customer the opportunity to use the Beta Version free of charge or sends him an Offer for paid use. Where WifOR sends an Offer, the Customer receives an access authorization for the number of users set out in the Offer, consisting of a username and a password.

3.3 Customer may process and reproduce the data and results derived from the Beta Version only to the extent that this is covered by the intended use of the Beta Version according to the current scope of functions provided in the Beta Version. Necessary reproduction includes the loading of the Beta Version into the RAM on WifOR's server, but not the even temporary installation or storage of the Beta Version on data carriers (such as hard disks or similar) of the hardware used by Customer.

3.4 Customer shall only be entitled to use the Beta Version for its own business activities by its own (also freelance) employees for the duration of this Agreement as intended.

4. Rights on materials provided for download

4.1 Customer has the possibility to use the Beta Version to visualize the results of analysis in predefined patterns and to download these results and visualizations (the "**Downloaded Materials**"). WifOR grants Customer a non-exclusive right, unlimited in time and space, to use the Downloaded Materials for its own purposes. This includes the right to reproduce, publish and distribute the visualizations, but not the right to edit the Downloaded Materials.

4.2 Watermarks or other references to WifOR in the Downloaded Materials may not be removed. When Downloaded Materials or parts thereof are used in presentations, articles, analyses, texts, and other publications, "WifOR" must always be cited as the source.

5. Obligations of the Customer

5.1 Customer shall keep the access data transmitted to him safe and protect it from access by third parties and keep it safe in accordance with state-of-the-art measures. Customer shall ensure that use only occurs to the contractually agreed extent. WifOR shall be notified immediately of any unauthorized access.

5.2 Customer is obligated not to store any data on the storage space provided by WifOR whose content or use violates applicable law, official orders, third-party rights or agreements with third parties.

- 5.3** Customer shall check its data for viruses or other harmful components before uploading, storing or using its data in the Beta Version and shall use state of the art measures (e.g., virus protection programs) for this purpose.
- 5.4** Customer is responsible for regularly making appropriate data backups, in particular to download the results obtained from using the Beta Version if further needed, e.g., for reasons of compliance documentation.
- 5.5** Customer grants WifOR the right to use and reproduce the uploaded data for the purposes of storage and access by the Customer, in particular to fulfill WifOR's contractual obligations to exploit its data with WifOR data.

6. General support and additional services

- 6.1** General support referring to the use of the Beta Version's functions is to be requested by Customer via email (impacttool@wifor.com) and provided by WifOR to Customer via e-mail, phone, and/or video call. Customer's requests for support are usually processed within 2 business days.
- 6.2** Additional services, such as training, comprehensive explanations of use that go beyond simple support requests, scientific consulting, functional extensions of the WifOR Impact Valuation Tool or the activation of additional users, are provided exclusively against separate remuneration and on the basis of a separate offer.

7. Confidentiality

- 7.1** "**Confidential Information**" means all information disclosed by a Party ("Disclosing Party") to the other Party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information of WifOR includes the content, functions, and know-how of the Beta Version as well as the WifOR data. Confidential Information of each Party shall include in particular, but not limited to business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such Party.
- 7.2** However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

7.3 As between the Parties, each Party retains all ownership rights in and to its Confidential Information. The Receiving Party shall use reasonable care to (i) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections materially similarly protective of the Confidential Information than those herein.

7.4 The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by mandatory applicable law or judicial or regulatory order to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted). The Receiving Party will provide reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

8. Processing of personal data

If Customer processes personal data within the scope of this Agreement, Customer is responsible for compliance with data protection laws. WifOR will process the data transmitted by Customer only within the scope of the instructions of Customer. If WifOR is of the opinion that an instruction of Customer violates data protection laws, WifOR will inform Customer thereof immediately. Details of commissioned data processing are dealt with in the **Annex 2** ("Data Processing Agreement").

9. Fees

9.1 Access to the free Beta Version is free of charge.

9.2 In case access is provided based on an individual Offer, Customer shall pay a fee to access the Beta Version as well as any additional fees for additional services as set out in the Offer.

9.3 All invoices shall be paid by Customer according to the terms and to the account indicated by WifOR in the Offer.

10. Liability; Indemnification

10.1 Both Parties shall be liable for damages – irrespective of the legal basis – in accordance with the statutory provisions in cases of:

- intent and gross negligence,
- slight negligence, with respect to damages to life, limb and health,
- malicious concealment of a defect, and
- Customer's claims pursuant to applicable product liability laws.

- 10.2** Without prejudice to subsection 10.1, the Party shall be liable for damages caused by a slightly negligent infringement of essential contractual obligations (*wesentliche Vertragspflichten*); essential contractual obligations are obligations which are essential for the proper fulfilment of the Agreement, which the other Party habitually relies and may rely on and which protect the essential legal positions of the other Party. However, in this case, Party's liability shall be limited to the typically foreseeable damage which is characteristic for such type of contract (*vertragstypisch vorhersehbarer Schaden*).
- 10.3** In the event of data loss or data destruction, a Party is only liable if the data loss or destruction was caused intentionally, through gross negligence or due to a breach of an essential contractual obligation by the respective Party. The amount of liability of the Party is limited to the damage that would have occurred if the other Party had properly backed up its data.
- 10.4** WifOR is in no case liable for misuse of the Beta Version by Customer.
- 10.5** Otherwise, the Party's liability – irrespective of its legal basis – shall be excluded. In particular, WifOR is not liable for lost profits, as well as not liable for defects that occur in connection with a change in the services by WifOR made by Customer or otherwise culpably caused by Customer or other external influences which originate from Customer's sphere of risk.
- 10.6** To the extent that WifOR's liability to Customer is limited or excluded, this applies *mutatis mutandis* to WifOR's legal representatives, employees, freelancers and other vicarious agents.
- 10.7** The liability for an only insignificant reduction in the suitability of the performance is excluded. The strict liability according to § 536a para. 1 Alt. 1 BGB for defects that already existed at the time of the conclusion of the Agreement is also excluded, insofar as it is not a defect of a property expressly warranted by WifOR.
- 10.8** WifOR shall indemnify Customer against all claims of third parties alleging that Customer's use of the Beta Version as agreed in this Agreement directly infringes the intellectual property rights or other rights of any third party, provided Customer promptly notifies WifOR in writing of the claim, provides its reasonable cooperation and information to WifOR and allows WifOR to have sole authority to control the defense and settlement of the third-party claim.

10.9 Customer shall indemnify WifOR against all costs, damages, and losses that WifOR may suffer as a result of Customer's breach of sections 5.1, 5.2, 5.3 and section 7 of this Agreement.

11. Term, Termination

11.1 This Agreement shall enter into force upon execution by both Parties or upon acceptance of the Customer's request for access to the free Beta Version by WifOR, and shall expire after one month, unless otherwise stated.

11.2 At the end of the Agreement, Customer's possibility of accessing the Beta Version shall end. The right of Customer to use the Downloaded Materials remains unaffected. Customer is obliged to save the data stored in the Beta Version in due time before the end of the term of this Agreement. All data of Customer will be irrevocably deleted no later than 90 days after the end of the term of the Agreement, unless they are subject to longer-term retention obligations of WifOR.

12. Miscellaneous

12.1 This Agreement, including any other documents referred to herein, constitutes the entire agreement and understanding among the Parties with respect to the subject matter hereof, and shall supersede all prior oral and written agreements or understandings of the Parties relating hereto.

12.2 Customer may only transfer rights and obligations arising from or in connection with this Agreement to third parties with the written consent of WifOR.

12.3 This Agreement (including this sub-section referring to the written form of amendments) may be amended only in writing by an amendment signed by both Parties.

12.4 If any part or provision of this Agreement is held invalid or unenforceable by any competent arbitral tribunal, court, governmental or administrative authority having jurisdiction, the other provisions of this Agreement shall nonetheless remain valid. In this case, the invalid or unenforceable provision shall be replaced (by an agreement among the Parties or court order, as the case may be) by a substitute provision that best reflects the economic intentions of the Parties without being unenforceable.

12.5 This Agreement shall in all respects be governed by, and construed in accordance with, German law to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods dated 11 April, 1980 and to the exclusion of conflict of law provisions.

12.6 The exclusive place of jurisdiction for all disputes arising from or in connection with the provision of services shall be Frankfurt am Main in the Federal Republic of Germany.

Annex

Annex 1 – License for Exiobase 3 dataset

Annex 2 – Data Processing Agreement

Annex 3 – License for FIGARO

Annex 1 to the General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool

The EXIOBASE 3 dataset is available for download at the following HYPERLINK and provided under the terms and conditions of the Attribution Share Alike 4.0 International Public License, which is accessible via the following HYPERLINK.

Cite as:

Stadler, Konstantin, Wood, Richard, Bulavskaya, Tatyana, Södersten, Carl-Johan, Simas, Moana, Schmidt, Sarah, Usubiaga, Arkaitz, Acosta-Fernández, José, Kuenen, Jeroen, Bruckner, Martin, Giljum, Stefan, Lutter, Stephan, Merciai, Stefano, Schmidt, Jannick H, Theurl, Michaela C, Plutzer, Christoph, Kastner, Thomas, Eisenmenger, Nina, Erb, Karl-Heinz, ... Tukker, Arnold. (2019). EXIOBASE 3 (3.7) [Data set]. Zenodo. <https://doi.org/10.5281/zenodo.3583071>

Please note that we have modified the data set for the purpose of the WifOR Impact Valuation Tool. For more information, please contact us via email: impacttool@wifor.com

Annex 2 to the General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool

Preamble

This Agreement details the Parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, and described in detail in the offer and the Agreement on Access to the Beta Version of the WifOR Impact Valuation Tool (hereinafter, the "**Principal Contract**"). Its regulations shall apply to any and all activities associated with the Principal Contract, in whose scope Processor's employees or agents process Company's personal data (hereinafter, "**Data**") on behalf of Company as a controller (hereinafter, "**Contract Processing**").

I Subject matter, duration and specification of contract processing of Data

- (1) The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Principal Contract. Specifically, Contract Processing shall include, but not be limited to, the following Data:

Type of data	Type and purpose (subject matter) of Contract Processing	Categories of data subjects affected
Names, e-mail addresses, telephone numbers, role, last login, and last IP address, current employer	Provision of the WifOR Impact Valuation Tool; (Login, Provision of additional services and support)	Employees of the Company

- (2) The Parties will each name a point of contact for all matters relating to the processing of Data.

II Scope of application and responsibilities

- (1) Processor shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Principal Contract. Within the scope of this Annex, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Processor and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.
- (2) Company's individual instructions on Contract Processing shall, initially, be as agreed in the Principal Contract. Company shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Processor. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

III Processor's obligations

- (1) Processor will arrange the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. Except where expressly permitted by Article 28 (3) (a) of the GDPR, Processor shall process data subjects' Data only within the scope of the Principal Contract and the instructions issued by Company. Where Processor believes that an instruction would be in breach of applicable law, Processor shall notify Company of such belief

without undue delay. Processor shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

- (2) Processor shall implement technical and organizational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Processor has implemented technical and organizational measures and safeguards these to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organizational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk. The measures taken at the time of the conclusion of the contract are listed in **Annex A**. Processor reserves the right to change the security measures taken, but it must be ensured that the contractually agreed level of protection is not undercut.
- (3) Processor shall, to the extent reasonable for the Processor, support Company in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. Insofar as the support results in efforts for Processor that are usually only provided against separate remuneration, Processor may claim remuneration usually demanded by Processor for such services.
- (4) Processor warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Processor's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Processor warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
- (5) Processor shall notify Company, without undue delay, if Processor becomes aware of breaches of the protection of Data within Processor's scope of responsibility. Processor shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Processor shall coordinate such efforts with Company without undue delay.
- (6) Processor shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Processor shall, based on Company's instructions, and unless agreed upon differently in the Principal Contract, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company. In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Principal Contract.
- (7) Processor shall, upon termination of Contract Processing and upon Company's instruction, return all Data, carrier media and other materials to Company or delete the same.
- (8) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Processor shall support Company in defending against such claims with reasonable effort.

IV Company's obligations

- (1) Company shall notify Processor, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Processor's work.
- (2) Section 3 para. 8 above shall apply, mutatis mutandis, to claims asserted by data subjects against Processor in accordance with Article 82 of the GDPR.

V Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Processor, and where Processor is able to correlate the data subject to Company, based on the information provided by the data subject, Processor shall refer such data subject to Company. Processor shall forward the data subject's claim to Company. Processor shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Processor shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

VI Options for documentation

- (1) Processor shall demonstrate to the Company compliance with the obligations set forth in this Annex by appropriate means; in particular, Processor shall provide the Company with the information and documents required to prove the obligations.
- (2) Company may obtain information from Processor, have existing test certificates from experts, certifications or internal audits presented to it or, if possible, inspect Processor's technical and organizational measures itself in person or have them inspected by a competent third party during normal business hours after timely coordination, provided that the third party is not in a competitive relationship with Processor. Company shall only carry out inspections to the extent necessary and shall not disproportionately disrupt Processor's operations in the process. Processor may make inspections dependent on prior notification with an appropriate lead time - as a rule at least 14 days - and on the signing of a declaration of confidentiality with regard to the data of other company's and the technical and organizational measures that have been set up. If the auditor commissioned by the Company is in a competitive relationship with Processor, Processor shall have a right of objection against the auditor.
- (3) In principle, auditors must be bound by a confidentiality obligation. It is not necessary to sign a confidentiality agreement if the supervisory authority or the auditor is subject to legal or professional confidentiality where a breach is punishable under the Criminal Code.
- (4) Each Party shall bear its own costs resulting from the audit. Company shall bear the costs for the use of an auditor commissioned by it.

VII Subcontractors (further processors on behalf of Company); Contractors outside the European Economic Area

- (1) Processor shall use subcontractors as further processors on behalf of Company only where approved in advance by Company.
- (2) Company hereby consents to Processor's use of subcontractors listed in **Annex B**. Processor shall, prior to the use or replacement of subcontractors, inform Company thereof. Company shall be entitled to contradict any change notified by Processor within a reasonable period of time and for materially important reasons. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, Company shall be entitled to terminating the Principal Contract.
- (3) Where Processor commissions subcontractors, Processor shall be responsible for ensuring that Processor's obligations on data protection resulting from the Principal Contract and this Annex are valid and binding upon subcontractor.
- (4) In the event of a transfer of Data to a subcontractor with its registered office in a country outside the European Economic Area (EEA) which does not guarantee an adequate level of data protection (unsafe third country), Processor shall ensure that this satisfies the requirements of Art. 44 et seq. GDPR, in particular that it has entered into or will enter into appropriate guarantees with the subcontractor within the meaning of the GDPR (e.g. conclusion of standard data protection clauses). Upon request, Processor shall provide the Company with evidence of the conclusion of the aforementioned agreements with its subcontractors.

VIII Liability and damages

- (1) Company and Processor shall be liable to data subject in accordance with Article 82 of the GDPR.
- (2) With respect to each other, Processor and Company shall only be liable if the breach lies within their own sphere of responsibility. In the event of a breach within the scope of joint responsibility, Processor and Company shall be liable to each other in proportion to their respective share of fault and/or responsibility.

IX Obligations to inform, mandatory written form, choice of law

- (1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Processor's control, Processor shall notify Company of such action. Processor shall notify to all pertinent parties in such action, that any Data affected thereby is in Company's sole property and area of responsibility, that Data is at Company's sole disposition, and that Company is the controller within the meaning of the GDPR.
- (2) No modification of this Annex and/or any of its components – including, but not limited to, Processor's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this Annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.
- (3) In case of any conflict, the data protection regulations of this Annex shall take precedence over the regulations of the Principal Contract. Where individual regulations of this Annex are invalid or unenforceable, the validity and enforceability of the other regulations of this Annex shall not be affected.
- (4) This Annex and its fulfilment are subject solely to the substantive law of the Federal Republic of Germany with the exception of the United Nations Convention on Contracts for the International Sale of Goods (CISG).

Annex A - Technical and organizational measures pursuant to Art. 32 of the GDPR

1. Confidentiality (Art. 32 Par. 1 lit. b GDPR)

- **Access control**
No unauthorized access to data processing equipment, e.g.: Magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;
- **Access control**
No unauthorized system use, e.g.: (strong) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media;
- **Access control**
No unauthorized reading, copying, modification, or removal within the system, e.g.: Authorization concepts and need-based access rights, logging of accesses;
- **Separation control**
Separate processing of data collected for different purposes, e.g., multi-client capability, sandboxing;
- **Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR).**
The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without recourse to additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

2. Integrity (Art. 32 para. 1 lit. b GDPR)

- **Disclosure control**
No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- **Input control**
Determining whether and by whom personal data has been entered into, modified or removed from data processing systems, e.g.: Logging, document management;

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

- Availability control;
- Protection against accidental or deliberate destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and contingency plans;
- Rapid recoverability (Art. 32(1)(c) GDPR);

4. Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR).

- Data protection management;
- Incident Response Management;
- Data protection-friendly default settings (Art. 25(2) GDPR);
- Contract control;
- No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g.: Clear contract design, formalized order management, strict selection of the service provider, prior conviction obligation, follow-up checks.

Annex B – Subcontractors

WifOR doesn't currently use any subcontractors for this purpose.

Annex 3 to the General Terms and Conditions on Access to the Beta Version of the WifOR Impact Valuation Tool

The source of FIGARO dataset is Eurostat.

FIGARO stands for 'Full International and Global Accounts for Research in input-Output analysis' and it is the result of a co-operation project between Eurostat and the Joint Research Centre of the European Commission. All data provided is available for download via the official Eurostat website (<https://ec.europa.eu/eurostat/web/main/home>).

The terms of use of Eurostat data are available under <https://ec.europa.eu/eurostat/web/main/about-us/policies/copyright>

Please note that we have modified the data set for the purpose of the WifOR Impact Valuation Tool. For more information, please contact us via email: impacttool@wifor.com