LIFESPIN GmbH – General Terms, July 2024

Effective as of 1 July 2024. These General Terms replace and supersede all prior versions.

1. Applicability.

1.1 **Applicability of these General Terms**. These terms of use ("**General Terms**") govern the agreement between lifespin GmbH, Germany ("**lifespin**" or "**we**") and the customer ("**Customer**" or "**you**") on the provision and delivery of results from the use of lifespin's analytical services by Customer ("**Main Agreement**"). If not explicitly stated otherwise, all services are for "Research Use Only" (RUO). These services may include one or more of the following: NMR measurement in lifespin's laboratory, metabolic data processing, artificial intelligence-driven analysis, and the reporting of data submitted by the Customer. The Main Agreement consists of these General Terms, the Customer's respective order form, and lifespin's order confirmation.

1.2 **Exclusion of conflicting terms**. These General Terms will apply exclusively. General terms and conditions of the Customer that deviate from or complement these General Terms will not become part of the Main Agreement, unless lifespin has explicitly agreed to them in text form. This also applies if lifespin provides the report or renders other services without rejecting the general terms and conditions of the Customer.

1.3 **Authorized Customers**. lifespin's services are available exclusively to commercial entities as defined in Sec. 14 of the German Civil Code, including public legal entities. lifespin's services are not intended for, nor available to, patients or consumers, and these General Terms do not apply to them.

2. Formation of Main Agreement.

2.1 **Offers**. All offers from lifespin, including those on the website, in advertisements, and in brochures, are non-binding and without obligation.

2.2 **Acceptance of Customer offers**. lifespin may accept offers from the Customer within three weeks of receipt. Amendments, modifications, or ancillary agreements require written confirmation in text format by lifespin to take effect.

3. Scope and time of performance obligation.

3.1 **Scope of performance obligation**. The scope of lifespin's obligations is primarily determined by the written or electronic order confirmation by lifespin. lifespin is authorized to use third parties to fulfill its contractual obligations.

3.2 **Approximate deadlines**. The deadlines and timeframes specified by lifespin are approximate unless expressly agreed otherwise. This means that after exceeding the specified non-binding date or timeframe, the Customer may formally request lifespin to perform within a reasonable period.

3.3 **Commencement of periods**. Delivery and performance periods generally commence upon the conclusion of the Main Agreement. If documents, samples or other data from the Customer, or other prerequisites (e.g. permits) are necessary for lifespin's performance the period shall only commence when these have been obtained by lifespin.

3.4 **Force majeure and delays**. If circumstances beyond lifespin's reasonable control, which may include acts of God, pandemics, embargoes, acts of war (including terrorist attacks), failure of a distributor, reseller or other supplier, labor disturbances and acts or regulations of governmental entities, impede, delay, or temporarily make impossible the performance of lifespin's service, lifespin is entitled to postpone the service by the duration of the impediment plus a

reasonable start-up period. If circumstances beyond lifespin's control permanently prevent the performance of the service, lifespin is entitled to withdraw from the Main Agreement in whole or in part.

3.5 **Extended impediments**. If the impediment (as described above in Section 3, clause 4) lasts longer than three months, the Customer is entitled to withdraw from the Main Agreement concerning the unperformed part after setting a reasonable grace period (*Nachfrist*).

3.6 **Client non-compliance**. If the Customer delays acceptance or culpably breaches other cooperative obligations, lifespin is entitled to seek compensation for any resulting damages, including additional expenses incurred.

4. Responsibilities of Customer. Customer shall

4.1 use commercially reasonable efforts to prevent unauthorized access to or use of the services, and notify lifespin promptly of any such unauthorized access or use;

4.2 use lifespin's services only in accordance with the Main Agreement, and all applicable laws and government regulations;

4.3 immediately inform lifespin about complaints or incidents in connection with lifespin's services; and

4.4 in the event of transmitting human samples and/or digitalized health data to lifespin,

(a) do so in a pseudonymized form, in compliance with all applicable data protection laws and regulations, ensuring that lifespin cannot trace these samples and/or digitalized health data back to the individual donor;

(b) obtain all necessary consents, permissions, or other authorizations required by law allowing lifespin to process human samples and/or digitalized health data of the donors for performing analytical services on a pseudonymized basis;

(c) inform donors about lifespin´s intent to reuse the human samples and/or digitalized health data for research and commercial purposes, specifically for the development and improvement of lifespin's analytical services, and endeavor to obtain consents for these use cases from the donors, if and to the extent required by law (it being understood that donors are not and cannot be obliged to provide such consent);

(d) transfer ownership of the transmitted samples to lifespin.

4.5 By placing an order, Customer confirms that it has obtained all necessary consents within the meaning of section 4.4(b). In addition, Customer informs lifespin if the respective donor has not provided the additional consent(s) within the meaning of section 4.4(c).

5. Samples.

5.1 **Costs and bearing of risk**. Unless otherwise agreed in the order confirmation, the submission of samples is at the expense and risk of the Customer.

5.2 **Sample delivery requirements**. Samples must be adequately packaged, labeled and delivered. The Customer is required to provide written or electronic notice of any hazardous, e.g., infectious, sample materials, as well as any known dangers and risks associated with the sample material before delivery. This also applies to risks associated with the storage of sample materials. lifespin reserves the right to refuse acceptance of hazardous sample materials unless explicitly committed to accept such hazardous materials.

5.3 **Remaining sample materials**. lifespin may store sample materials in its biodata bank upon completion of sample processing, unless the Customer expressly objects prior to the initial sample delivery. In the event of such objection, Customer may choose to collect the remaining sample material at Customer's expense or to ask lifespin to dispose of it following consultation with lifespin.

6. Storage of data. Unless otherwise agreed, data not subject to statutory retention periods will be stored free of charge for up to 12 months. Upon consultation with the Customer, these data may be further stored at the Customer's expense.

7. Pricing and taxes.

7.1 **Pricing.** All prices for services are in Euros.

7.2 **Taxes.** Applicable taxes, customs duties, import fees, handling charges, regulatory fees, and other mandatory charges, if any, are additional.

8. Payment; offsetting, withholding.

8.1 **Payment terms**. Unless otherwise agreed, lifespin's invoices are due immediately upon Main Agreement execution and payable within 14 days of invoice receipt without any deduction. lifespin is entitled to deliver performance results (e.g., test reports, analysis results) concurrently with payment of the agreed price.

8.2 **Creditworthiness**. If the Customer fails to meet payment conditions, or if post-contract circumstances become known to lifespin that materially reduce the Customer's creditworthiness and, in lifespin's estimation, jeopardize the realization of its claims, lifespin is entitled to withdraw from Main Agreements already concluded with the Customer unless the Customer, upon lifespin's request, makes an advance payment or provides other security as chosen by lifespin.

8.3 **Default interest**. In the event of payment delay, lifespin is entitled, without further reminder, to charge interest on overdue amounts at 9 percentage points above the basic interest rate per annum as per Section 247 of the German Civil Code, but at least 10% of the overdue amount per annum. The right to claim higher damages for delay is reserved.

8.4 **Right to setoff and withholding**. The Customer is entitled to set off or retain payment only if its counterclaims are undisputed or have been legally established. Furthermore, the Customer may assert a right of retention only if its counterclaim and lifespin's claim arise from the same contractual relationship.

9. Customer Accounts and communication preferences.

9.1 **Customer Account**. To access and use certain services, you may need to register for a Customer Account ("**Customer Account**"). If you register for a Customer Account, you must provide accurate account information and promptly update this information if it changes. You also must maintain the security of your Customer Account and promptly notify us if you discover or suspect that someone has accessed your Customer Account without your permission. If you permit others to use your Customer Account credentials, you are responsible for the activities of those users that occur in connection with your Customer Account.

9.2 **Suspension or termination by lifespin**. lifespin may, at any time, terminate or suspend your right to use and access the Customer Account if: (a) you breach any provision of the General Terms (or act in a manner that clearly shows you do not intend to, or are unable to, comply

with the General Terms); (b) you fail to make the timely payment for the services; (c) we are required to do so by law (for example, where the provision of the services to you is, or becomes, unlawful); or (d) we elect to discontinue the services, in whole or in part (such as if it becomes impractical for us to continue offering services in your region due to change of law). If we terminate your right to use and access the Customer Account other than for cause, we will make reasonable efforts to notify you at least 30 days prior to termination via the email address you provide to us.

9.3 **Electronic communications**. By creating a Customer Account, to the extent required by applicable law, you also consent to receive electronic communications from lifespin (e.g., via email). These communications may include operational notices about the Customer Account (e.g., password changes and other transactional information) and are part of Customer's relationship with lifespin. Customer agrees that any notices, agreements, disclosures or other communications that lifespin sends electronically will satisfy any legal communication requirements, including, but not limited to, that such communications be in text form. lifespin may also send Customer promotional communications via email, including, but not limited to, newsletters, special offers, surveys and other news and information about similar lifespin products and services, provided that Customer did not object. Customer may at any time object to receiving these promotional emails, without incurring any transmission costs other than those in accordance with basic rates. To this end, Customer may follow the unsubscribe instructions provided in those emails.

10. Intellectual property rights.

10.1 **Ownership of Intellectual Property**. lifespin owns and retains all rights, title and interest in and to the services, and all other technology, software, algorithms, documentation, user interfaces, trade secrets, techniques, designs, inventions, text, reports, dashboards, analyses, graphics, images, photographs, videos, illustrations, trademarks, trade names, service marks, logos, slogans, works of authorship and other tangible and intangible material, content and information pertaining thereto or included therein ("**lifespin IP**"). All intellectual and industrial property rights in or to the lifespin IP, including patents, copyrights, and inventor rights, are and will remain the exclusive property of lifespin or its licensors, whether or not specifically recognized or perfected under the laws of the jurisdiction in which the lifespin IP are used or licensed. Customer will not take any action that jeopardizes lifespin's or its licensors' proprietary rights, or attempt to acquire any right, in the lifespin IP. All rights not expressly granted to Customer with respect to lifespin IP are reserved by lifespin and its third-party licensors. Unless otherwise agreed on a case-by-case basis, lifespin will own all rights, including intellectual and industrial property rights, in any copy, translation, modification, improvement, adaptation, derivative work or other derivation of the lifespin IP. Customer will execute, or will at lifespin's request procure the execution of, any instrument that may be appropriate to assign these rights to lifespin to perfect these rights in lifespin's name. Customer shall not alter or remove any trademarks applied to, embedded in or associated with, the lifespin IP.

10.2 **Use of trademarks and proprietary rights**. The Customer may use trademarks, trade names, other designs, and proprietary rights of lifespin only with prior written or electronic permission and solely in the interest of lifespin.

10.3 **Third-party rights**. The Customer is responsible for ensuring that lifespin's contractual performance, based on instructions and contributions from the Customer such as the provision of sample materials, does not infringe third-party intellectual property rights. The Customer shall indemnify lifespin from all third-party claims related to the infringement of such intellectual property rights, including all related legal and extrajudicial costs.

11. lifespin liability.

11.1 **Limitation of liability**. lifespin's liability is unlimited in case of mandatory statutory liability, including: (a) liability resulting from death or personal injury caused by negligence or willful misconduct, (b) any other liability resulting from an intentional or grossly negligent breach of duty, (c) liability under the German Product Liability Act, and any other laws that expressly provide that liability cannot be excluded or relieved in advance, and (d) liability based on an independent warranty promise, or the assumption of strict liability. In all other cases, lifespin's liability for damages shall be limited as follows:

(a) lifespin shall only be liable for damages caused by a slightly negligent breach of a material contractual obligation up to the amount of the typically foreseeable damages at the time of entering into these Terms.

(b) lifespin shall not be liable for damages caused by a slightly negligent breach of a non-material contractual obligation.

(c) Material contractual obligation means an obligation without which proper execution of the contract is impossible, and that can be relied on by parties to this agreement.

11.2 **No liability for Customer-provided items**. lifespin assumes no liability for samples, materials, components, shipping instructions, processing guidelines, or similar items provided by the Customer unless expressly agreed otherwise in writing. lifespin is not obligated to inspect these items. In case of defects, the Customer bears full liability and shall indemnify lifespin from all third-party claims in their entirety.

11.3 **No liability for Customer's AI literacy.** lifespin assumes no liability for the adequacy of Customer's staff or other individuals in possessing the necessary skills, knowledge, and understanding of artificial intelligence required for informed deployment of lifespin's services. This includes awareness of the risks associated with artificial intelligence and the ability to avoid making unverified decisions.

12. Customer data; Privacy.

12.1 **Customer data**. The parties assume that the data transmitted by the Customer to lifespin are not subject to intellectual property right protection. Should any intellectual property right protection nonetheless exist or arise in the future regarding this data, the Customer hereby grants lifespin a non-exclusive, worldwide, perpetual (i.e., continuing after termination of the Main Agreement), royalty-free license to copy, aggregate, compile, modify, and use the data submitted by the Customer to lifespin in connection with the services, as necessary for lifespin to provide the services, perform its obligations, and exercise its rights under the Main Agreement, including using the collected data for the purpose of continuously training and developing lifespin's technology. This includes the right to incorporate the data into other data collections and databases of lifespin, to combine, edit, and use it within lifespin's technology. This also includes the right of public access. The provider is authorized to modify the results and to use the modified results in the same manner as the original. lifespin may use the data for any purpose permitted by applicable law. If the results are eligible for patent or copyright protection, the Customer shall receive reasonable compensation for the transfer or use of its results by lifespin, which the parties shall agree upon separately.

12.2 **Data Protection; Data Processing Agreement**. To the extent the Customer data comprises personal data (as defined under any EEA laws and regulations applicable to the processing of personal data, including Regulation (EU) 2016/679 of 27 April 2016 (GDPR) as may be amended), lifespin and Customer each recognize that they have full and entire knowledge of the obligations

under applicable data protection laws that apply to (a) Customer and lifespin as independent data controllers in order to manage their business contacts for the purposes of their reciprocal commercial and contract management relationship, (b) Customer as independent data controllers for the purposes of performing its professional practice, (c) lifespin as data processor where lifespin performs, on behalf of Customer and under Customer's instructions, the processing of personal data for the performance of analytical services; and (d) lifespin as independent data controller when reusing the personal data for research and commercial purposes. For the purposes of (c) above, Customer and lifespin agree to the Data Processing Agreement in Exhibit A.

13. Confidential Information. Except as otherwise required or permitted in the Main Agreement, neither party will use or disclose the other party's Confidential Information without the other party's prior written consent. "Confidential Information" means any information, whether disclosed orally, in writing, electronically, visually or otherwise by one party to the other in the course of the Main Agreement, including, all information relating to the party's financial condition, operations, business or customers. Each party will use the same degree of care as it exercises toward its own Confidential Information in protecting the other party's Confidential Information, but no less care than reasonable in light of general industry standards and applicable laws regarding data protection, privacy or confidentiality. Confidential Information will only be disclosed on a need-to-know basis to a party's employees and contractors bound by non-disclosure obligations at least as protective as those of the Main Agreement. This Section 13 does not apply to information (a) after it becomes publicly known through no fault of the receiving party, (b) already rightfully in the receiving party's possession on a non-confidential basis when received, (c) developed by the receiving party without the use of the other party's Confidential Information or (d) is rightfully received by the receiving party on a non-confidential basis after the receipt of such information under the Main Agreement. If any Confidential Information is required to be disclosed by law, the receiving party shall give the disclosing party immediate notice of the request or order (to the extent permitted by applicable law) that the Confidential Information be disclosed and the fullest opportunity under law to prevent or limit the disclosure. Each party acknowledges that its breach of this Section 13 may cause the other party substantial and irreparable harm for which the other party would be entitled to seek injunctive relief, if applicable, in addition to any available legal remedies. Each party hereby waives, as a condition to receiving such relief, any requirement to post bond or provide other security. For clarity, lifespin Confidential Information includes lifespin IP, and Customer Confidential Information does not include personal data.

14. Applicable law, jurisdiction, and place of performance.

14.1 **Governing law**. These General Terms and all legal relations between lifespin and the Customer are governed by the laws of the Federal Republic of Germany, without regard to conflict of law rules.

14.2 **Jurisdiction**. Any disputes arising out of or in connection with the Main Agreement (including non-contractual disputes or claims) is subject exclusively to the jurisdiction of the court in the district where lifespin has its principal office, namely Regensburg, Germany. lifespin reserves the right to bring a lawsuit at the Customer's principal place of business.

14.3 **Place of performance**. Unless otherwise provided by law, the place of performance for all claims arising from the Main Agreement is lifespin's registered office.

15. Miscellaneous.

15.1 **Assignment**. Customer may not assign any rights or delegate any obligations under the Main Agreement without the prior written consent of lifespin. Any attempted assignment or delegation by Customer in violation of this Section 15.1 will be null and void. This does not apply to

the assignment of claims to monetary payments; however, lifespin may make payment to the previous creditor with discharging effect.

15.2 **Severability; Beneficiaries**. If any term of the Main Agreement is held to be unenforceable, the other terms of the Main Agreement will be enforced to the fullest extent permitted by law. No person or entity other than lifespin and Customer have any rights under the Main Agreement.

15.3 **Waiver**. No waiver or failure of a party to assert any right under the Main Agreement on any one occasion will operate as a waiver of the same or any other right on any other occasion.

15.4 **Notices**. You may send notices to us at Am BioPark 13, 93053 Regensburg, Germany. We may notify you by email, postal mail, postings within the services, or other legally accepted means. It is your responsibility to keep your account information current to receive notifications.

15.5 **Export and Import Laws**. Export laws and regulations of the European Union, United States and other relevant local export laws and regulations may apply to the services provided under the Main Agreement. Customer agrees that such export control laws govern Customer's use of the services (including technical data) and any lifespin material, and Customer agrees to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). Customer agrees that no data, information, program and/or materials resulting from use of the services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws.

15.6 **Conflicting Languages**. If these General Terms are translated into any language other than English, and there is a discrepancy between the English version and the translated text, the English version will govern unless expressly stated otherwise in the translation.

Exhibit A
DATA PROCESSING AGREEMENT
pursuant to Article 28 GDPR

between

Customer

as Controller

– hereinafter referred to as "**Customer**" –

and

lifespin GmbH, Am BioPark 13, 93053 Regensburg Germany,

as Processor

– hereinafter referred to as "**Supplier**" –

Supplier and Customer may hereinafter also be referred to individually as a "**Party**" or together as "**Parties**".

Preamble

This Exhibit details the Parties' obligations on the protection of personal data, associated with the processing of personal data on behalf the Controller, and described in detail in General Terms.

1. Subject of the Agreement

(a) This Data Processing Agreement (hereinafter "Agreement") governs the processing of personal data under the General Terms. In the course of rendering bioanalytical services it is necessary that the Supplier deals with personal data with regard to which the Customer acts as a controller in terms of data protection law (hereinafter referred to as "**Customer Data**").

(b) With this Agreement, the Parties specify supplier´s obligations under the General Data Protection Regulation ("GDPR"). The provisions of this Agreement shall apply to each activity the Supplier performs on behalf of the customer in connection with the General Terms and which involves or may involve the processing of personal data in the sphere of customer.

(c) The services provided by Supplier under the General Terms may include NMR measurement in a laboratory, metabolic data processing, artificial intelligence-driven analysis, and the reporting of human sample data submitted by the Customer. Supplier only processes personal data, including health data, on the documented instructions of Customer and in accordance with the General Terms.

2. Definitions

2.1 Unless otherwise stated in this Agreement, the terms used herein shall have the meaning given to them in Art. 4 GDPR.

2.2 "Health Data" means personal data relating to the physical or mental health status of the Donor, including human samples.

2.3 "Services" means the bioanalytical services in accordance with the General Terms and Conditions.

2.4 “Subcontractors” means any entity which provides services to supplier which include processing of personal data.

2.5 “Supervisory Authority” means (a) an independent public authority which is established by a member state of the European Union pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Legislation.

3. Subject and scope of the commissioning

3.1 The Supplier shall process the Customer Data on behalf and in accordance with the instructions of the Customer within the meaning of Art. 28 GDPR (Processing on Behalf). The Customer remains the controller in terms of data protection law.

3.2 The processing of Customer Data by the Supplier occurs in the manner and the scope and for the purpose determined in Annex 1 to this Agreement; the processing relates to the types of personal data and categories of data subjects specified therein. The duration of processing corresponds to the term of the Main Agreement.

3.3 The processing of Customer Data by the Supplier shall in principle take place inside the European Union or another contracting state of the European Economic Area (EEA). The Supplier is nevertheless permitted to process Customer Data in accordance with the provisions of this agreement outside the EEA if he informs the Customer in advance about the place of data processing and if the requirements of Art. 44 to 48 GDPR are fulfilled or if an exception according to Art. 49 GDPR applies.

4. Right of the Customer to issue instructions

4.1 The Supplier processes the Customer Data in accordance with the instructions of the Customer, unless the Supplier is required to do so by Union or Member State law to which the Supplier is subject. In the latter case, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 The instructions of the Customer are in principle conclusively stipulated and documented in the provisions of this Agreement. Individual instructions which deviate from the stipulations of this Agreement or which impose additional requirements shall require the Supplier's consent. The instruction must be documented and the assumption of any additional costs incurred by the Supplier as a result must be guaranteed by the Customer.

4.3 The Supplier shall ensure that the Customer Data is processed in accordance with the instructions given by the Customer. If the Supplier is of the opinion that an instruction given by the Customer infringes this Agreement or applicable data protection law, he is after correspondingly informing the Customer entitled to suspend the execution of the instruction until the Customer confirms the instruction. The Parties agree that the sole responsibility for the processing of the Customer Data in accordance with the instructions lies with the Customer.

5. Obligations and legal status of the Customer

5.1 The Customer is solely responsible for the permissibility of the processing of the Customer Data and for safeguarding the rights of data subjects in the relationship between the Parties. Should third Parties assert claims against the Supplier based on the processing of Customer Data in accordance with this Agreement, the Customer shall indemnify the Supplier from all such claims upon first request.

5.2 The Customer is responsible to provide the Supplier with the Customer Data in time for the rendering of services and he is responsible for the quality of the Customer Data. The Customer shall inform the Supplier immediately and completely if during the examination of the of the Supplier's results he finds errors or irregularities with regard to data protection provisions or his instructions.

5.3 On request, the Customer shall provide the Supplier with the information specified in Art. 30 para. 2 GDPR, insofar as it is not available to the Supplier himself.

5.4 If the Supplier is required to provide information to a governmental body or person on the processing of Customer Data or to cooperate with these bodies in any other way, the Customer is obliged at first request to assist the Supplier in providing such information and in fulfilling other cooperation obligations.

6. Requirements for personnel and systems/Confidentiality

6.1 The Supplier shall ensure that, pursuant to Art. 29 GDPR, all persons under its authority process the Customer Data in accordance with this Agreement, as well as the instructions of the Customer.

6.2 The Supplier shall commit all persons engaged in processing Customer Data to confidentiality with respect to the processing of Customer Data.

7. Security of processing

7.1 The Supplier takes according to Art. 32 GDPR necessary, appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Customer Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Customer Data appropriate to the risk. These are listed in Annex 2.

7.2 The Supplier shall have the right to modify technical and organizational measures during the term of the Agreement, as long as they continue to comply with the statutory requirements.

8. Engagement of further processors

8.1 The Customer grants the Supplier the general authorization to engage further processors with regard to the processing of Customer Data. Further processors consulted at the time of conclusion of the agreement result from Annex 3. In general, no authorization is required for contractual relationships with service providers that are concerned with the examination or maintenance of data processing procedures or systems by third parties or that involve other additional services, even if access to Customer Data cannot be excluded, as long as the Supplier takes reasonable steps to protect the confidentiality of the Customer Data.

8.2 The Supplier shall notify the Customer of any intended changes in relation to the consultation or replacement of further processors. In individual cases, the Customer has the right to object to the engagement of a potential further processor. An objection may only be raised by the Customer for important reasons which have to be proven to the Supplier. Insofar as the Customer does not object within fourteen (14) days after receipt of the notification, his right to object to the corresponding engagement lapses. If the Customer objects, the Supplier is entitled to terminate the Main Agreement and this Agreement with a notice period of three (3) months.

8.3 The agreement between the Supplier and the further processor must impose the same obligations on the latter as those incumbent upon the Supplier under this Agreement. The Parties agree that this requirement is fulfilled if the contract has a level of protection corresponding to this Agreement, respectively if the obligations laid down in Art. 28 para. 3 GDPR are imposed on the further processor.

8.4 Subject to compliance with the requirements of Section 3.5 of this Agreement, the provisions of this Section 8 shall also apply if a further processor in a third country is involved. The Parties agree in this case that the requirements of Section 8.3 above are met if the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the EU Commission Decision of 4 June 2021 (“Standard Contractual Clauses”) are concluded with the further processor in the third country. The Customer declares his willingness to cooperate in fulfilling the requirements of Art. 49 GDPR to the extent necessary.

9. Data subjects' rights

9.1 The Supplier shall support the Customer within reason by virtue of technical and organizational measures in fulfilling the latter's obligation to respond to requests for exercising data subjects' rights.

9.2 As far as a data subject submits a request for the exercise of his rights directly to the Supplier, the Supplier will forward this request to the Customer in a timely manner.

9.3 The Supplier shall inform the Customer of any information relating to the stored Customer Data, about the recipients of Customer Data to which the Supplier shall disclose it in accordance with the instruction and about the purpose of storage, as far as the Customer does not have this information at his disposal and as far as he is not able to collect it himself.

9.4 The Supplier shall, within the bounds of what is reasonable and necessary, against reimbursement of the expenses and costs incurred by the Supplier as a result of this and to be proven enable the Customer to correct, delete or restrict the further processing of Customer Data, or at the

instruction of the Customer correct, block or restrict further processing himself, if and to the extent that this is impossible for the Customer.

9.5 Insofar as the data subject has a right of data portability vis-à-vis the Customer in respect of the Customer Data pursuant to Art. 20 GDPR, the Supplier shall support the Customer within the bounds of what is reasonable and necessary in return for reimbursement of the expenses and costs incurred by the Supplier as a result of this and to be proven in handing over the Customer Data in a structured, commonly used and machine-readable format, if the Customer is unable to obtain the data elsewhere.

10. Notification and support obligations of the Supplier

10.1 Insofar as the Customer is subject to a statutory notification obligation due to a breach of the security of Customer Data (in particular pursuant to Art. 33, 34 GDPR), the Supplier shall inform the Customer in a timely manner of any reportable events in his area of responsibility. The Supplier shall assist the Customer in fulfilling the notification obligations at the latter's request to the extent reasonable and necessary in return for reimbursement of the expenses and costs incurred by the Supplier as a result thereof and to be proven.

10.2 The Supplier shall assist the Customer to the extent reasonable and necessary in return for reimbursement of the expenses and costs incurred by the Supplier as a result thereof and to be proven with data protection impact assessments to be carried out by the Customer and, if necessary, subsequent consultations with the supervisory authority pursuant to Art. 35, 36 GDPR.

11. Deletion and return of Customer Data

11.1 After the end of the provision of services relating to processing, the Supplier shall delete the Customer Data, unless the Supplier is obligated by Union or Member State law to further store the Customer Data.

11.2 The Supplier may keep documentations, which serve as evidence of the orderly and accurate processing of Customer Data, also after the termination of the Agreement.

12. Evidence and audits

12.1 The Supplier shall provide the Customer, at the latter's request, with all information required and available to the Supplier to prove compliance with his obligations under this Agreement.

12.2 The Customer or another auditor mandated by the Customer shall be entitled to audit the Supplier with regard to compliance with the provisions of this Agreement, in particular the implementation of the technical and organizational measures; including inspections.

12.3 In order to carry out inspections in accordance with Section 12.2., the Customer is entitled to access the business premises of the Supplier in which Customer Data is processed within the usual business hours (Mondays to Fridays from 10 a.m. to 6 p.m.) after timely advance notification in accordance with Section 12.5 at his own expense, without disruption of the course of business and under strict secrecy of the Supplier's business and trade secrets.

12.4 The Supplier is entitled, at his own discretion and taking into account the legal obligations of the Customer, not to disclose information which is sensitive with regard to the

Supplier's business or if the Supplier would be in breach of statutory or other contractual provisions as a result of its disclosure. The Customer is not entitled to get access to data or information about the Supplier's other customers, cost information, quality control and contract management reports, or any other confidential data of the Supplier that is not directly relevant for the agreed audit purposes.

12.5 The Customer shall inform the Supplier in good time (usually at least two weeks in advance) of all circumstances relation to the performance of the audit. The Customer may carry out one audit per calendar year. Further audits are carried out against reimbursement of the costs and after consultation with the Supplier.

12.6 If the Customer commissions a third party to carry out the audit, the Customer shall obligate the third party in writing the same way as the Customer is obliged vis-à-vis the Supplier according to this Section 12 of this Agreement. In addition, the Customer shall obligate the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional obligation of secrecy. At the request of the Supplier, the Customer shall immediately submit to him the commitment agreements with the third party. The Customer may not commission any of the Supplier's competitors to carry out the audit.

12.7 At the discretion of the Supplier, proof of compliance with the obligations under this Agreement may be provided, instead of an inspection, by submitting an appropriate, current opinion or report from an independent authority (e.g. auditor, audit department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit - e.g. according to BSI-Grundschutz - (“audit report”), if the audit report makes it possible for the Customer in an appropriate manner to convince himself of compliance with the contractual obligations.

13. Contract term and termination

The term and termination of this Agreement shall be governed by the term and termination provisions of the Main Agreement. A termination of the Main Agreement automatically results in a cancellation of this Agreement. An isolated termination of this contract is excluded.

14. Liability

14.1 The Supplier's liability under this Agreement shall be governed by the disclaimers and limitations of liability provided for in the Main Agreement. As far as third parties assert claims against the Supplier which are caused by the Customer's culpable breach of this Agreement or one of his obligations as the controller in terms of data protection law affecting him, the Customer shall upon first request indemnify and hold the Supplier harmless from these claims.

14.2 The Customer undertakes to indemnify the Supplier upon first request against all possible fines imposed on the Supplier corresponding to the Customer's part of responsibility for the infringement sanctioned by the fine.

15. Final provisions

15.1 In case individual provisions of this Agreement are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The Parties undertake to replace

the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.

15.2 The Agreement will be governed by the same law as the General Terms, and the competent courts agreed between the Parties under the General Terms shall have the sole jurisdiction concerning all conflicts arising out of or in connection with the Agreement as well.

15.3 No modification or amendment of this Agreement shall be effective unless in writing.

15.4 This Agreement is an exhibit to the General Terms and supplements the General Terms.

15.5 In case of conflicts between this Agreement and other arrangements between the Parties, in particular the Main Agreement, the provisions of this Agreement shall prevail.

16. Appendices to this Agreement

The following appendices are an integral part of this Agreement:

APPENDIX 1 Data Processing Activities

APPENDIX 2 Data protection concept / technical and organizational measures of lifespin

APPENDIX 3 Subcontractors

APPENDIX 1

Data Processing Activities

1. **Categories of data subjects whose personal data will be processed**

   Donors (typically patients treated by Customer)

2. **Categories of personal data processed**

   On behalf of Controller, lifespin processes donor´s personal data, including health and genomic data for the purpose of lifespin's Services.

2.1. Personal data

Personal master data (name, address, date of birth, sex, ethnicity, weight and height, menstrual cycle, general lifestyle (smoker/non-smoker, sportive activity, consumption of alcohol/drugs, nutrition)

2.2. Health data

metabolome profile, medication, anamnesis data, diseases, co-mobirdities, clinical chemistry data, other diagnostic data

2.3. Genetic Data

human samples, including blood samples

3. **Data processing activities**

   Depending on the occasion, collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission or otherwise making available, alignment or combination, erasure or destruction.

4. **Purpose(s) of the data processing on behalf of the Controller**

   lifespin processes Health Data for bioanalytical services which comprise:
   - Nuclear Magnetic Resonance (NMR) measurement in a laboratory
   - metabolic data processing
   - artificial intelligence-driven analysis
   - the reporting of human sample data submitted by Customer

5. **Duration of the Data Processing**

   Identical with term of General Terms of Use.

APPENDIX 2

Data protection concept / technical and organizational measures of Processor

This document describes the technical and organizational measures implemented by lifespin to meet legal and contractual requirements when processing personal data, in particular those set out in Article 32 para 1 GDPR. The following measures apply to all data processing activities that are under control of lifespin, or where lifespin is a subcontracted data processor on behalf of another data controller.

lifespin reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that lifespin processes.

1. Confidentiality according to Art. 32 para. 1 (b) GDPR

1.1. Access control

Access control describes measures that prevent unauthorised persons from gaining access to processing systems with which data processing is carried out.

Technical measures
☒ Automatic access control system
☒ Manual or mechatronic locking system
☒ Workplace computers are in locked rooms
☒ Doors with knobs on the outside
☒ Barrier/sliding gate for vehicles
☒ Photoelectric sensors/ Light barriers / motion detectors
☒ Security and locking service for properties outside operating hours
☒ Measures to prevent easy eavesdropping and viewing (especially for customer reception, shared spaces, or mobile working)

Organisational measures
☒ Documented key management
☒ Closing control
☒ Entry / Reception / Gatekeeper
☒ Practised regulations for the access of external persons (e.g. escorts, access bans, ID cards)

1.2. Data carrier and memory control

Data carrier control describes measures that prevent the unauthorised reading, copying, modification or deletion of data carriers. Storage control describes measures to prevent the unauthorised input, access, modification and deletion of stored personal data.

Technical measures
☒ Logging of the deletion/destruction of data carriers
☒ Logging of the destruction of paper

Organisational measures
☒ Secure storage of mobile data carriers

Encryption acc. to Art. 32 para. 1 (a) GDPR
☒ All encryption technologies used in production are state of the art

1.3. User control

User control describes measures to prevent the use of automated processing systems using data transmission equipment by unauthorised persons. This can also include protection against unauthorised system use and against system intrusion and misuse via networks.

Technical measures
☒ Use of an anti-virus solution on client computers and notebooks with daily updates of the signature databases
☒ Use of an endpoint protection system on client computers and notebooks, including automatic on-access scans
☒ Use of an anti-virus solution or an endpoint protection system on servers
☒ Use of an anti-virus solution or endpoint protection system on smartphones and tablets
☒ Checking incoming emails using anti-malware protection
☒ Use of Intrusion Prevention System (IPS)
☒ Wireless access only via current WLAN routers with effective access mechanisms
☒ Guest WLAN without access to the internal network
☒ Only software for which security updates are made available in a timely manner is used
☒ Use of operating systems and software for which security updates are still available
☒ No mobile devices are used for which there are no (or no longer any) security updates.
☒ Automatic rollout of security-relevant updates and patches for operating systems from client computers
☒ Proper configuration of software distribution services
☒ Configuration of automatic security updates for servers
☒ Prompt manual installation of security updates on risk-prone servers
☒ Use and proper configuration of a hardware and software firewall
☒ Configuration of demilitarised zones

1.4. Access control

Access control describes measures to ensure the exclusive use of automated processing systems by authorised persons under the scope of their access authorisation and thus guarantees that authorised persons only have access to data covered by their authorisation.

Technical measures
☒ Login with username & password
☒ Use of biometric features for login on IT devices or in security zones (e.g. fingerprint, FaceID, etc.)
☒ For smartphones: access only after authentication (e.g. PIN, password)
☒ Only strong passwords are used for the admin accounts of the IT systems (e.g. at least 16 characters, complex and without common word components).
☒ No dependency of the entire operation on individual employees with administrator IDs.
☒ Secure storage of central administration access data (e.g. in a safe) and access options in an emergency.
☒ Use of different administration roles with rights according to the least privilege principle for different administration tasks (e.g. software updates, configuration, backup).
☒ Publication of password rules for employees (e.g. prohibition of disclosure, storage in the browser or multiple use)
☒ Password manager in use
☒ Automatic blocking of access in the event of too many failed attempts (temporarily or completely)

Organisational measures
☒ Centralized password assignment
☒ Default authentication information assigned by the manufacturer is changed after installation
☒ Management of user rights by the IT administrator
☒ Secure delivery of login information for users (e.g. encrypted e-mail, separate letters for user name and password)
☒ Passwords are blocked after a security incident, even if suspected, and must be reassigned by the user.
☒ Documented authorisation concept including role profiles for employees to control, regulate and manage access to information.
☒ Regularly check whether the assignment of roles corresponds to the specifications and whether the roles still meet the requirements of the business activity.
☒ Number of IT administrators reduced to a minimum

1.5. Separability

Separability describes measures that ensure that personal data collected for different purposes can be processed separately.

Technical measures
☒ Implementation of client separation through separation at data level
☒ Carry out suitable network segmentation: Restrictive (physical) separation of sensitive networks (e.g. medical networks in hospitals or personnel administration) from administrative networks (using firewall systems).

Organisational measures
☒ Authorization concept
☒ Separation of access using database rights

1.6 Pseudonymisation acc. to Art. 32 para. 1 (a) GDPR

Pseudonymization describes measures so that the data can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is separately kept and is subject to corresponding technical and organizational measures. Applying pseudonymization to personal data can reduce the risks to the data of the data subjects. Pseudonymisation is sufficient if de-pseudonymisation by internal users is not possible or only possible with disproportionate effort.

Technical measures
☒ Pseudonymisation through assignment tables, these are separated from the rest of the data processing.

Organisational measures
☒ Separation of the pseudonymising body from the data user or separation of the assignment data in separate and secure IT systems
☒ Multi-level pseudonymisation by different actors if necessary
☒ Secure, centralised management and monitoring of cryptographic keys, pseudonymisation keys or mapping tables

2. Integrity according to Art. 32 para. 1 (b) GDPR

2.1. Transmission and transport control

The transmission control describes measures for checking the addressee of the data transmission. Transport control describes measures to ensure the confidentiality and integrity of data when transporting data carriers.

Technical measures
☒ Transport encryption is implemented only end-to-end.
☒ For messengers: Use of state-of-the-art transport and content encryption of messages and files
☒ Use of encrypted and password-protected data containers (e.g. ZIP, RAR file)
☒ No usage of unencrypted protocols (e.g. FTP, Telnet) when transferring personal data
☒ Connection of branch offices only via VPN connections
☒ Remote maintenance of clients for administrative purposes exclusively via encrypted connections after authentication by the administrator and release by the user

Organisational measures
☒ The access of service providers to your own systems via remote maintenance is fully logged
☒ Careful selection of transport personnel and vehicles
☒ Secure transport containers/packaging
☒ For physical transport: personal handover with protocol

2.2. Input control

Input control describes measures for (retrospective) verification of which personal data has been entered or modified in automated processing systems, at what time and by whom.

Technical measures
☒ Traceability of data entry, modification and deletion through personalised (unique) identifiers in IT applications

2.3 Reliability & data integrity

Reliability describes measures that ensure that all system functions are available and that any malfunctions that occur are reported. Data integrity ensures that stored personal data cannot be damaged by system malfunctions.

Technical measures
☒ Regularly updated firewall and network components

☒ Regular updates of the spam filter
☒ Regular updates of the the virus scanner
☒ Regularly check that the firewall is configured correctly (e.g. by scanning ports for your own IP addresses)
☒ Encryption of the databases of IT applications with critical data

3. Availability and resilience of the systems (resilience) according to Art. 32 para. 1 (b) GDPR

3.1 Recoverability acc. to Art. 32 para. 1 (c) GDPR

Recoverability describes measures that ensure that deployed systems can be restored in the event of a fault.

☒ Documented backup policy for servers and end devices
☒ Checking the data backup process
☒ Regular data recovery tests and logging of the process (recommendation: quarterly)
☒ Suitable physical storage of backup media in a secure location outside the server room (e.g. safe, fire protection, physical separation)

3.2 Availability control

Availability control describes measures that ensure that personal data is protected against accidental destruction or loss.

Technical measures
☒ Server rooms and/or data centres have fire extinguishers or fire extinguishing systems
☒ Server rooms and/or data centres have sufficient air conditioning
☒ Use of systems to ensure the power supply to server systems (UPS), especially in the event of short-term power failures or fluctuations
☒ Server rooms and/or data centres have protective socket strips
☒ RAID system / hard drive mirroring
☒ In server rooms that are shared with other companies, hardware (interfaces) are secured by locked racks, locked cabinets or similar
☒ Physical protection of the server room against break-ins
☒ No risks from flooding/heavy rain, especially for server rooms in the basement
☒ Physical protection of the router

Organisational measures
☒ Up-to-date device management and documentation is available.
☒ Fire protection concept

4. Procedures for regular review, assessment and evaluation according to Art. 32 para. 1 (d) GDPR

Organisations must not only implement appropriate security measures, but also ensure that these measures are reviewed and evaluated at regular intervals. This process should ensure that the measures taken continue to be effective and meet current requirements in order to minimise data protection risks.

Organisational measures
☒ Conclusion of data processing agreements with subcontractors in accordance with Art. 28 GDPR
☒ Review of technical and organisational measures in accordance with Art. 32 GDPR
☒ Centralised documentation of all procedural instructions and regulations on data protection with access for employees as required
☒ Documented process for recognising, reporting, handling, and following up on security and data protection incidents.
☒ Documentation of security and data protection incidents (e.g. ticket system)
☒ Regular review, assessment, and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing

5. Security of the development environment

5.1 Software development

Data protection and security must be considered at an early stage in the development of in-house software systems or when selecting software products for your own company.

Technical measures
☒ Separation of productive from the development/test systems
☒ Access to source code in software development is restricted
☒ Ongoing inventory of the versions of software or components (e.g. frameworks, libraries) and their dependencies
☒ Standard software and corresponding updates are only obtained from trustworthy sources

Organisational measures
☒ Documentation of own IT applications (system description, authorisation concept, interfaces, reports, deletion concept)
☒ No storage of personal data or access data in the source code management
☒ Data entries are validated according to semantic criteria (semantic input validation)
☒ Purpose attributes have been defined and implemented for data fields and records
☒ Only synthetic data, i.e. no real data or personal data, is processed in the test and development environment.
☒ Relevant employees are trained that security by design (ensuring confidentiality, availability, and integrity) as a subset of data protection by design is a legal data protection requirement and has an influence on central design decisions (product selection, centralised vs. decentralised, pseudonymisation, encryption, country of a service provider)
☒ Sufficient test cycles are considered

☒ Ensure that an ongoing plan is in place to monitor, evaluate and apply updates or configuration changes for the life of a software application

5.2 Development of web applications (e.g. online shop, apps, etc.)

Websites and web applications are usually easily accessible platforms for attacks, which can usually be well secured using known best-practice approaches.

Technical measures
☒ There is a separation of the production system from the development/test system
☒ The database of the online application (e.g. online shop) is sufficiently encrypted according to the state of the art.
☒ Remote access to web servers is only possible with an encrypted connection and two-factor authentication (e.g. SSH with client certificates).
☒ A RAID system / hard drive mirroring is used
☒ Web application firewall (WAF) or web service firewall for web applications

Organisational measures
☒ If content is not to be found by a search engine (via robots.txt), the respective content has been blocked from being found by search engines.
☒ Data entries are validated according to semantic criteria (semantic input validation).
☒ Purpose attributes have been defined and implemented for data fields and records.
☒ Only synthetic data, i.e. no real data or personal data, is processed in the test and development environment.
☒ No personal data or access data is stored in the source code management.
☒ Employees are trained in the fact that security by design (ensuring confidentiality, availability, and integrity) as a subset of data protection by design is a legal data protection requirement and has an influence on central design decisions (product selection, centralised vs. decentralised, pseudonymisation, encryption, country of a service provider).

6. Ensuring processing in accordance with instructions pursuant to Art. 32 para. 4 GDPR

These measures protect data security against internal compromise and reduce the risk of circumvention of the technical security measures by the natural persons entrusted with data processing.

Organisational measures
☒ IT guideline for users
☒ Regulations on the mobile/private use of end devices (e.g. smartphones, notebooks) by employees are in place.
☒ Home office guideline
☒ Confidentiality obligation for clients
☒ Confidentiality obligation for contractors
☒ Confidentiality agreements for employees
☒ Onboarding process for employees
☒ Offboarding process for employees

APPENDIX 3

Subcontractors appointed by lifespin

KKIT Kernkompetenz-IT Systemhaus GmbH
Adalbert-Stifter-Straße 45
93051 Regensburg

Auvaria Technology GmbH
Warschauer Pl. 11-13
10245 Berlin

Softloop GmbH
Lindleystr. 8a
60314 Frankfurt am Main