Publishing Agreement

SPRINGER NATURE

This Publishing Agreement (the "**Publishing Agreement**") for the journal titled

npj Viruses

is made between

Springer Nature Limited
The Campus, 4 Crinan Street, London N1 9XW, United Kingdom
(the "**Publisher**")

on the one hand and

World Society for Virology
1 Envelope Terrace, Unit 115, Worcester, MA 01604, USA
represented by: Prof. Maria Söderlund-Venermo, President and Prof. Marietjie Venter, President - Elect
(the "**Organisation**")

on the other hand.

For good and valuable consideration, the parties agree as follows:

1. Definitions

In this Publishing Agreement, unless the context otherwise requires, the following words and expressions will have the following meanings:

APC	means the Journal's Article Processing Charge.
Commencement Date	means 01 January 2026.
Journal	means a professional journal titled *npj Viruses* including all material published in, or in relation to, such professional journal and all or any part of this professional journal such as articles, abstracts, indexes, text, illustrations, images, bibliographic and other data, supplements, special editions and any further content contained therein.

LTP	means the Publisher's standard Licence To Publish agreement for articles accepted for publication in the Journal.
Parties	means the Publisher and the Organisation (each a "**Party**").
Term	has the meaning ascribed to it in the Clause "**Term**".

2. Publication

As owner of the Journal, the Publisher will publish and distribute the Journal in accordance with its practices and procedures as determined by the Publisher from time to time.

3. Designation of the Journal

At all times during the Term, the Journal will be designated by the Organisation as an affiliated publication of the Organisation. The Journal's website will refer to the Organisation affiliation, and the Publisher will appropriately acknowledge the Journal as an affiliated publication of the Organisation in major promotional activities of the Journal.

4. Intellectual Property Rights

4.1 The Parties acknowledge that all intellectual property rights in the Journal, including the title of the Journal and all associated goodwill are, and will remain, the sole and exclusive property of the Publisher except as expressly otherwise provided in this Publishing Agreement.

4.2 For clarity, nothing in this Publishing Agreement is to be construed to transfer to the Organisation, or give the Organisation a claim of ownership over, any intellectual property rights in anything provided or created by or on behalf of the Publisher and used in, or in connection with, the Journal (including the layout, domain name and software).

5. Rights Granted to the Publisher

5.1 If and to the extent that the Organisation provides the Publisher with content to be published in the journal, e.g. Organisation news, commentary and other material ("**Organisation Material**"), the Organisation grants to the Publisher a non-exclusive, perpetual, worldwide, irrevocable, assignable and sub-licensable right to publish, produce, copy, distribute, communicate, display publicly, commercialise, and/or otherwise make the Organisation Material and/or any part thereof available in any language, in any and all forms, and/or media of expression, whether now known or developed in the future, including in connection with any and all end-user devices, and using any publishing and distribution models, in each case with the right to grant further time-limited or permanent rights.

5.2 The above grant includes the following rights in respect of the Organisation Material:

a) the right to edit, alter, adapt, adjust and prepare derivative works (e.g. databases, compilations, anthologies, abridged versions, offprints, reprints, etc.);

b) all advertising, promotional and marketing rights including in relation to social media;

c) rights for any training, educational and/or instructional purposes (including massive open online courses);

d) the right to add and/or remove links or combinations with other media/works; and

e) the right to store and archive the Organisation Material.

5.3 The Publisher may exercise any of the above rights either directly or indirectly via third parties.

5.4 The Organisation hereby grants to the Publisher the right to create, use and/or license and/or sub-license content data and/or metadata of any kind in relation to the Organisation Material or parts thereof without restriction.

5.5 Subject to the terms and conditions of this Publishing Agreement, the Organisation hereby grants to the Publisher for the Term a non-exclusive licence to use the name of the Organisation and any registered or unregistered rights in signs, trademarks, trade names, designs, layout or logotypes associated with the Organisation in connection with the exercise of its rights as the Publisher of the Journal.

6. Responsibilities of the Publisher

6.1 As between the Parties, the Publisher will be responsible for and will have the sole right to determine in its sole discretion:

a) all matters relating to production and distribution of the Journal;

b) the design and layout for the Journal in all media, including the cover design (the "**Journal Design**");

c) copy-editing and production of the Journal in all formats in line with the Publisher's in-house copy-editing style manual, which may be changed from time to time; and

d) the planning, implementation and management of the promotion, marketing and advertising of the Journal to appropriate worldwide markets, subject to discussion with the Organisation from time to time.

6.2 The Publisher will provide to the Organisation on request an annual report regarding the Journal's development.

6.3 The Publisher will advertise conferences organised by the Organisation on the Journal's website in the announcement section of the homepage.

6.4 As a service to authors, peer reviewers and editors, the Publisher may in its sole discretion provide support for the transfer of scientifically valid manuscripts that are rejected from one journal to other journals in the Springer Nature group portfolio more appropriate for the manuscript ("**Transfer Service**").

6.5 The Publisher reserves the right to amend or replace its online platforms, brands, imprints, systems, workflows and rights forms as it deems appropriate in its sole discretion, as long as this does not prevent the Publisher from fulfilling its obligations under this Publishing Agreement.

6.6 Notwithstanding the foregoing, or any other provision of this Publishing Agreement, the Publisher reserves the right to:

a) refuse to publish all or any part of the Journal;

b) edit, annotate, suspend, withdraw, correct or retract all or any part of the Journal; or

c) take any other remedial action in relation to all or any part of the Journal;

in each case where the Publisher has grounds to believe that failing to do so could result in liability for or damage to the Publisher or otherwise having an adverse impact upon the Journal. In such circumstances, the Publisher will consult with the Organisation and the Editor-in-Chief over the action taken.

7. Open Access Fee

7.1 The Parties acknowledge that the Publisher or an affiliate will charge an APC for each article accepted for publication in the Journal.

7.2 The APC will either be borne by the respective corresponding author or covered by funding, sponsorship, membership or other APC payment arrangements ("**Arrangements**"). The Publisher will have the right to grant discounts for such Arrangements.

7.3 The Publisher will offer a 15% discount to the then-current APC for authors whose articles are editorially accepted for publication in the Journal and for whom the Organisation confirms, through the process set out further below in this Clause "**Open Access Fee**" that they are members of the Organisation.

7.4 The Organisation will not charge any additional fee to any author of an editorially accepted article in connection with the online publication of the article.

7.5 As part of the publication process, authors will have the option to identify themselves on the Publisher's platforms as authors eligible for an APC discount ("**Affiliated Authors**").

7.6 The Publisher shall notify the Organisation by email each time an author has identified

themselves as an Affiliated Author.

7.7 The Organisation shall confirm or deny that the author is an Affiliated Author within three business days following such notification. In the event that the Publisher does not receive either a confirmation or a denial within four business days after the Publisher has notified the Organisation, the Publisher will send a reminder to inform the Organisation that following a four-day grace period the Publisher will deem the author not to be an Affiliated Author and that it will apply the General APC Conditions as specified in this Clause "**Open Access Fee**". An author for whom the Organisation has confirmed the status as an Affiliated Author shall be eligible for an APC discount ("**Eligible Author**").

7.8 For the process of notification and verification the Organisation shall nominate and register an OA contact ("**Verifying OA Contact**") with the Publisher not later than 30 days prior to the Effective Date. The Organisation may authorise the Editor(s)-in-Chief, or another Editorial Board member, of the Journal to act on behalf of the Organisation as Verifying OA Contact in the process of verifying authors as Eligible Authors. The Organisation will update the Publisher with respect to such authorisations and required details, such as the email address of the Verifying OA Contact, without undue delay. The Publisher shall set-up the Organisation-nominated person as Verifying OA Contact within 30 days after receipt of the Organisation's nomination by e-mail.

7.9 Authors who do not have sufficient funds to pay the APC may request a discretionary full or partial waiver, with eligibility for such waivers being dependent on the ability of authors to demonstrate a genuine lack of funds. Responsibility for administering requests for APC waivers will rest with the Publisher.

7.10 The Publisher will in every calendar year waive the APCs for up to four articles submitted for publication in the Journal ("**Annual APC Waivers**"). The selection of these articles will be made at the discretion of the Organisation and will be communicated to the Publisher by the Journal's Editor(s)-in-Chief. The Organisation, the Publisher and the Journal's Editor(s)-in-Chief will strive to align such Annual APC Waivers with the overall development plan for the Journal.

8. Data Protection

8.1 The Parties are independent data controllers and each of them warrants that it will comply with all applicable data protection laws (each as amended or replaced from time to time) including the General Data Protection Regulation (EU) 2016/679 together with any national laws implementing the same ("**Data Protection Laws**").

8.2 With regard to the processing and control of personal data the Parties agree to complete and execute the data transfer agreement in the form as set out in the **Appendix** "**Data Protection**" at the same time as signing this Publishing Agreement.

8.3 The Parties will not transfer any personal data received from the other party to outside

the EEA unless the transferor: (i) ensures the transfer is to a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; (ii) participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Parties can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Data Protection Legislation; or (iii) the transfer complies with the Data Protection Legislation.

9. Content Platform(s)

9.1 The Journal will be published via the Publisher's content platform(s) or any other electronic format or means of electronic distribution provided by or through the Publisher.

9.2 Additional electronic supplementary material may be published on the Publisher's content platform(s) if technically and financially feasible and if such material is related and linked to articles published in the Journal. Such supplementary material may include illustrations, datasets, video, and other scientific material related to the aims and scopes of the Journal.

10. Supplements

10.1 The Journal may publish abstract and full-paper supplements (the "**Supplements**"), subject to approval by the Journal's Editor-in-Chief. The Publisher retains the sole right to establish and levy publication charges for such Supplements and to invoice for such charges.

10.2 Waivers or individual discounts to APCs will not be available for abstracts. In addition, articles accepted for publication in such Supplements, and charges for Supplements or individual articles in Supplements may not be covered through an Arrangement.

10.3 Notwithstanding the foregoing, Supplements originating from meetings affiliated with the Organisation (the "**Meeting-Supplements**") are entitled to a discount of 20% off the Publisher's standard charges applicable to Supplements.

11. Advertising

11.1 The Publisher and its media representatives (including external agencies) have the sole right to: (i) solicit advertising to appear in the Journal or on the content platform(s) hosting the Journal; (ii) establish rates for such advertisements; and (iii) invoice for such advertisements.

11.2 If a prospective advertiser approaches the Organisation, it will refer such prospective advertiser to the Publisher.

12. Term

This Publishing Agreement will become effective upon the Commencement Date and will remain in full force until 31 December 2030 ("**Term**"), subject always to earlier termination in accordance with the Clause "**Termination**".

13. Termination

13.1 Without prejudice to any other right or remedy available to it, either Party ("**Notifying Party**") may immediately terminate this Publishing Agreement by written notice if at any time:

a) a supervisor, receiver, administrator, administrative receiver or other encumbrancer is appointed for the notified Party ("**Notified Party**") or takes possession over a substantial part of its property or assets;

b) the Notified Party becomes or threatens to become insolvent or is unable to pay its debts as they become due or makes any arrangement or compromise with or for the benefit of its creditors;

c) the Notified Party seeks relief, or if proceedings are commenced against the Notified Party or on its behalf, under any bankruptcy, insolvency or debtor's relief law, and those proceedings have not been vacated or set aside within 60 days from the date of their commencement;

d) the Notified Party is liquidated or dissolved, ceases or threatens to cease to carry on its business or operations, or is otherwise unable to perform fully under this Publishing Agreement; or

e) the Notified Party suffers or permits any analogous event to the foregoing in relation to it under the laws of the country in which it is incorporated or established.

13.2 Without prejudice to any other right or remedy available to it, the Notifying Party may immediately terminate this Publishing Agreement by written notice if:

a) at any time the Notified Party commits a material breach of its obligations under this Publishing Agreement which, if such breach is remediable, the Notified Party fails to remedy within 30 days of written notice from the Notifying Party requiring it to do so;

b) the Notified Party repeatedly commits breaches of its obligations under this Publishing Agreement such that the Notifying Party cannot reasonably be expected to continue the contractual relationship until the end of the Term; or

c) in the circumstances described in and in accordance with the procedures set out in the Clause titled "**Force Majeure**".

13.3 Without prejudice to any other right or remedy available to it, the Publisher may immediately terminate this Publishing Agreement by written notice to the Organisation if at any time:

a) the Organisation is in material breach of any applicable anti-bribery and/or corruption laws or any other law, the Publisher's Business Partner Code of Conduct , or is otherwise in material breach of accepted ethical standards in research and scholarship, or becomes the subject of any sanction issued in any applicable jurisdiction, or by its involvement with the Journal have caused or would be likely to cause an adverse impact on the reputation of the Journal and/or the Publisher (including through accusations of their unlawful or inappropriate behaviour);

b) the Organisation materially or repeatedly fails to cooperate in good faith and in a timely manner with the Publisher in relation to any reasonable queries, concerns, disputes, claims or legal action that might arise from or in connection with the publication of the Journal or fails to give the Publisher access at reasonable times to any relevant accounts, documents and records within the possession or control of the Organisation.

14. Representations and Warranties

14.1 Each Party represents and warrants that:

a) it has the right and authority to enter into and perform its obligations under this Publishing Agreement and neither execution nor performance of this Publishing Agreement will cause it to be in breach of any other agreement to which it is a party or of any laws or regulations; and

b) the person(s) executing this Publishing Agreement on its behalf has/have the demonstrable right and authority to do so and once so executed, this Publishing Agreement will constitute the legal, valid and binding obligation of such Party.

14.2 In addition, the Organisation represents and warrants that:

a) no material provided by the Organisation for publication in the Journal, including any promotional or advertising material and any pages offered to the Organisation for announcements and other information will infringe any copyright, database right, trade secret, moral right, trademark or patent or obligation of confidentiality or violate any other intellectual property or other right of any person or entity or contain any matter that may cause religious or racial hatred or encourage terrorism or unlawful acts, or be defamatory (or contain malicious falsehoods), invade any right of privacy or publicity or infringe data protection law, or be otherwise actionable, including under any action related to any injury resulting from the use of any practice or formula disclosed in the Journal;

b) no person acting on behalf of the Organisation has directly or indirectly: (i) paid,

provided, offered or authorised any payment, gift, inducement or other benefit to any person including any governmental or regulatory entity or official in any territory for the purpose of improperly obtaining, retaining or directing business or to secure or obtain any improper business advantage; nor (ii) received, accepted or authorised any such benefit from any such person for any such purpose;

c) no person acting on behalf of the Organisation will directly or indirectly commit any of the prohibited actions set out in subclause (b) above at any time during the Term (and during the term of any renewal agreement).

14.3 At all times the Organisation will comply in full with:

a) all applicable anti-bribery and corruption laws and regulations;

b) all applicable modern anti-slavery and labour laws;

c) all applicable data protection (as defined below in the Clause "**Data Protection**") and electronic privacy and marketing laws and regulations;

d) the Publisher's Business Partner Code of Conduct as amended from time to time and currently available online at http://www.springernature.com/businesspartnercodeofconduct-EN (in case of a material amendment the Publisher will inform the Organisation accordingly and, without written objection within 30 days, the amended version will be considered as accepted; in each case the Publisher will inform the Organisation that its silence will constitute a consent); and

e) all other laws and regulations applicable to the business of professional journals.

Notwithstanding any other provision of this Publishing Agreement, any breach by the Organisation of this Clause may be regarded by the Publisher as incapable of remedy and permitting the Publisher, without prejudice to its other rights and remedies, to terminate this Publishing Agreement with immediate effect by written notice.

15. Indemnification

15.1 The Organisation will indemnify and hold harmless the Publisher, any affiliated companies of the Publisher and the Publisher's sub-contractors from and against any loss, damage, cost, expense (including reasonable, actual and documented legal fees), recovery, judgment, award or claim of any kind arising from any breach or alleged breach of any of the Organisation's representations or warranties under this Publishing Agreement.

15.2 The Publisher will indemnify and hold harmless the Organisation from and against any loss, damage, cost, expense (including reasonable, actual and documented legal fees), recovery, judgment, award or claim of any kind arising from any breach or alleged breach of any of the Publisher's representations or warranties under this Publishing

Agreement.

15.3 Each Party's indemnification obligation is subject to the following conditions: (i) the Party seeking indemnification (the "**Indemnified Party**") will promptly inform the indemnifying Party (the "**Indemnifying Party**") in writing of any matter of which it becomes aware which may give rise to the Indemnifying Party's indemnification obligation, and the Parties will cooperate in good faith to seek to mitigate the impact of such matter; (ii) the Indemnified Party will not make any admission of liability, or enter into any agreement or compromise in relation to the matter without the prior written consent of the Indemnifying Party (such consent not to be unreasonably withheld, conditioned or delayed); (iii) unless agreed otherwise with the Indemnified Party, the Indemnifying Party will have the conduct of any defence of the matter with counsel of its own selection; (iv) the Indemnified Party will reasonably cooperate with the Indemnifying Party in such defence (and may join in such defence with counsel of its own selection, at its own expense); and (v) after consultation with the Indemnified Party and due consideration of any objections such Party may have, the Indemnifying Party may settle any such matter in its sole discretion.

16. Limitation of Liability

16.1 Nothing in this Publishing Agreement limits or excludes any liability for:

a) death or personal injury caused by negligence; or

b) fraud or fraudulent misrepresentation; or

c) any other liability which cannot be limited or excluded by applicable law or regulation.

Each Party's liability arising under or in connection with Clauses "**Representations and Warranties**" and "**Indemnification**" will not be limited.

16.2 Neither Party shall be liable to the other for any of the following types of loss or damage even if, in each case, it is advised of the possibility of such loss or damage: special, indirect or consequential loss; pure economic loss, costs, damages or charges; loss of profits; loss of revenue; loss of contracts; loss of anticipated savings; loss of business; loss of use; loss of goodwill; and loss or damage arising from loss, damage or corruption of any data.

16.3 Subject to subclause 1 of this Limitation of Liability Clause, the Publisher's total liability to the Organisation, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with this Publishing Agreement will be limited to the greater of EUR 12,000 or 125% of the amount paid or payable under this Publishing Agreement in the 12 months preceding any such liability claim.

17. Confidentiality

17.1 With respect to either Party, "**Confidential Information**" will mean confidential or proprietary information maintained by that Party as confidential. Tangible forms of Confidential Information must be clearly marked as "confidential" or "proprietary" at the time of disclosure. Any information that is disclosed orally or visually must be designated as "confidential" or "proprietary" at the time of disclosure or with written confirmation within 30 days following disclosure.

For the avoidance of doubt, the terms of this Publishing Agreement are deemed Confidential Information.

17.2 Neither Party ("**Recipient**") will disclose or use any Confidential Information of the disclosing Party ("**Disclosing Party**") other than in connection with the exercise of its rights and fulfilment of its obligations under this Publishing Agreement, and for its own internal administrative purposes, unless:

a) the Recipient received the Confidential Information from sources lawfully permitted to disclose it, free from any confidentiality restrictions;

b) the Confidential Information has been made available to the public by a person or entity not bound by a confidentiality restriction and other than through the recipient;

c) the Confidential Information was known to the Recipient prior to disclosure by the Disclosing Party to this Publishing Agreement, its representatives or agents;

d) the Confidential Information was independently developed by the Recipient without reference to, or reliance on, disclosure by the Disclosing Party to this Publishing Agreement, its representatives or agents of the Confidential Information; or

e) the recipient is required to make such a disclosure by applicable law or at the direction of a court or governmental agency, but only to the extent that it is legally obliged to do so, and after the Disclosing Party has been given a reasonable opportunity to obtain a protective order or similar relief, where legally permissible.

18. Force Majeure

Neither Party will be liable for its delay or failure to perform to the extent caused by circumstances beyond its reasonable control, including fire, flood, strike, terrorism, pandemic, action or inaction of civil, governmental or military authority, or acts of God. Without prejudice to any other right or remedy available to it, either Party may immediately terminate this Publishing Agreement by written notice if at any time the Notified Party is delayed in performing or fails to perform its obligations under this Publishing Agreement by circumstances as described in this Clause for a period of at least 45 days.

19. Relationship of Parties

At all times in connection with this Publishing Agreement, the Parties will be independent contractors and nothing in this Publishing Agreement will create a relationship of agency or partnership or a joint venture. Accordingly, neither Party will be authorised to bind the other save as expressly permitted by the terms of this Publishing Agreement.

20. Notices

All notices must be provided in writing in the English language and delivered by post, courier or personal delivery addressed to the physical address of the Notified Party as set out at the beginning of this Publishing Agreement or any replacement address notified to the Notifying Party for this purpose. All such notices will become effective upon receipt by the Notified Party. Notwithstanding the foregoing, notices sent by post or left at the address by courier or personal delivery, without evidence of receipt, will be deemed to have been received five working days after the notice was sent by post or delivered, as the case may be. A copy of any notice of breach, termination notice or other notice requesting remediable action to the Publisher will be sent to the Publisher's Legal Department located at The Campus, 4 Crinan Street, London N1 9XW, United Kingdom. Without limiting the foregoing, notification by e-mail will not be deemed effective service in any legal action, including arbitrations.

21. Taxation

21.1 All amounts mentioned in this Publishing Agreement are exclusive of any value added or similar taxes ("**VAT**"), government fees or levies or other assessments (together referred to as "**Taxes**"). Reporting, collection and/or remittance of such Taxes to the relevant tax authority will be the responsibility of the Party who has the legal obligation to do so.
If VAT is chargeable/due, the payer will pay to the payee (in addition to and at the same time as paying the principal amounts) an amount equal to the amount of such VAT. Appropriate invoices as required by law will be issued.

21.2 If there is a legal requirement for the Publisher to withhold any Taxes ("**Withholding Taxes**"), the Withholding Taxes will be deducted by the Publisher from the payments to the Organisation. Withholding Taxes, if any, will be borne by the Organisation. The Publisher will arrange for timely remittance of the Withholding Taxes in the minimum amount required by law and report related information to the competent tax authorities. The Publisher will provide the Organisation with appropriate proof of the remittance upon request by the Organisation. In case a reduction/exemption of Taxes can be claimed (e.g. on the basis of a tax treaty), the Organisation will provide the Publisher with sufficient proof to enable the Publisher to take into consideration the reduction or exemption. Where necessary, the Publisher will cooperate with the Organisation to arrange for such a reduction/exemption.

22. Governing Law and Jurisdiction

If any dispute arises between the Parties concerning the meaning of this Publishing Agreement or the rights and liabilities of the Parties, the Parties will engage in good faith discussions to attempt to seek a mutually satisfactory resolution of the dispute. This Publishing Agreement will be governed by, and will be construed in accordance with, the laws of England and Wales. The courts of London, UK will have the exclusive jurisdiction.

23. General Provisions

23.1 In this Publishing Agreement, any words following the terms “include”, “including”, “in particular”, “for example”, “e.g.” or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

23.2 No failure or delay by a Party to exercise any right or remedy provided under or in connection with this Publishing Agreement, nor any partial exercise of such right or remedy, will constitute a waiver of that or any other right or remedy, nor will it prevent or restrict the further exercise of that or any other right or remedy.

23.3 This Publishing Agreement will be binding upon and inure to the benefit of the successors and assigns of the Publisher. No Party will assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Publishing Agreement without prior written consent. Notwithstanding the foregoing, the Publisher may assign or transfer any or all of the rights and obligations under this Publishing Agreement to (i) an affiliate or (ii) any party acquiring substantially all the assets of the Publisher or of the part of the Publisher’s business which publishes the Journal, without the prior written consent of the Organisation.

23.4 This Publishing Agreement may not be modified or amended except by written agreement of the Parties. If one or more provisions of this Publishing Agreement are held to be unenforceable under applicable law, each such provision will be excluded from this Publishing Agreement and the balance of the agreement will be interpreted as if that provision were so excluded. This Publishing Agreement constitutes the entire agreement and understanding between the Parties in respect of its subject matter and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations, undertakings or understandings between them (whether written or oral) made before the Commencement Date relating to its subject matter.

23.5 Each Party agrees that it will have no remedies in respect of any statement, representation, assurance, undertaking or warranty (whether made innocently or negligently) that is not expressly set out in this Publishing Agreement.

23.6 This Publishing Agreement does not confer any rights on any third party (other than the successors and/or permitted assigns of the Parties, where applicable).

23.7 The Parties agree that electronic signature using an industry accepted electronic signature service such as DocuSign will constitute valid and binding signature for all purposes under this Publishing Agreement.

23.8 The Clauses "**Indemnification**", "**Limitation of Liability**", "**Confidentiality**", "**Force Majeure**", "**Governing Law and Jurisdiction**", and "**General Provisions**" will survive the expiration or prior termination of this Publishing Agreement.

The Parties have signed this Publishing Agreement to indicate their agreement to the terms set forth herein.

Signed for and on behalf of the Organisation
World Society for Virology

Signed by:
Prof. Maria Söderlund-Venermo
06A72E0591CD491...

08 January 2026

.....

Prof. Maria Söderlund-Venermo
President

.....

Signing Date

Signed by:
Prof. Marietjie Venter
E122E5C03A9A410...

12 January 2026

.....

Prof. Marietjie Venter
President - Elect

.....

Signing Date

Signed for and on behalf of the Publisher
Springer Nature Limited

Signed by:
Scott Rae
41D7D48AB3B44DD...

06 January 2026

.....

Scott Rae
Senior Publishing Manager

.....

Signing Date

DocuSigned by:
Joe Bennett
4F1C9BDAC1FC43B...

08 January 2026

Joe Bennett
Director, Publishing Strategy

Signing Date

_____

For internal use only:
Journal Number: 44298
GPU/PD/PS/Date of draft creation: PU 74 – Nature Portfolio/721/5537/24 October 2025
Legal Entity Number: 1267
44298_npj Viruses_SNOwned_AffSoc_24 October 2025_World Society for Virology_English Only – Contract Express V.1.7.7 (08_2025)-269590

Appendix – Data Protection

SCC – Controller-to-Controller

The parties listed in Annex I conclude the "standard contractual clauses" as set out in the COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) in the version of

- MODULE ONE, Controller-to-Controller-transfers -

I. The parties specify the open issues in the body of these standard contractual clauses as follows:

Clause 17 - Governing law:

The Parties agree on OPTION 1 (choice of law in any EU Member State). The governing law shall be the law of the Federal Republic of Germany.

Clause 18 (b) - Choice of forum and jurisdiction:

The Parties agree that any dispute arising from these standard contractual clauses shall be resolved by the courts of Berlin, Germany.

II. The parties agree upon the exclusion of the optional docking clause - **Clause 7** - into these standard contractual clauses.

III. The parties agree upon the exclusion of the option of allowing data subjects to lodge a complaint with an independent dispute resolution body in **Clause 11 (a)**.

IV. The Parties agree upon following inclusions in the appendix of the standard contractual clauses:

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s):

Name: Springer Nature Limited
Address: The Campus, 4 Crinan Street, London, N1 9XW, United Kingdom
Contact person's name, position and contact details: Joe Bennett, Director, Publishing Strategy, Springer Nature Limited, The Campus, 4 Crinan Street, London N1 9XW, United Kingdom

Activities relevant to the data transferred under these Clauses: *Publishing*

Signature:

Date: DocuSigned by: Joe Bennett 4F1C9BDAC1FC43B... 08 January 2026

Role (controller/processor): *Controller*

Data importer(s):

Name: World Society for Virology
Address: 1 Envelope Terrace, Unit 115, Worcester, MA 01604, USA
Contact person's name, position and contact details: Prof. Maria Söderlund-Venermo, President, World Society for Virology, 1 Envelope Terrace, Unit 115, Worcester, MA 01604, USA

Activities relevant to the data transferred under these Clauses: *Responsibilities of the Organisation as defined in the Publishing Agreement*

Signature:

Date: Signed by: Prof. Maria Söderlund-Venermo 06A72E0591CD491... 08 January 2026

Role (controller/processor): *Controller*

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

- Authors

- Peer reviewers
- Editorial board members
- Editors
- Organisation members (in case of member subscriptions)
- Subscribers
- Registrants of Table-of-Content (TOC) alerts (and other email services)

Categories of personal data transferred

- Generally: Name, surname, email address and affiliation
- Specifically for peer reviewers: Name, surname, email address, affiliation and peer review record with Publisher, as well as area of expertise
- Specifically for authors: Name, surname, email address, affiliation and relationship record with data exporter if applicable, as well as area of expertise
- Specifically for Organisation members: Name, surname, email address for receiving TOC alerts notifying members of the latest journal issue
- Where applicable for print copies – subscribers physical address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

☐ One-off transfer ☒ Transfer on a continuous basis ☐ Multiple on demand

Nature of the processing

- For publishing of the journal as defined in the Publishing Agreement

Purpose(s) of the data transfer and further processing

- To provide peer review data to the Editors of the journal **npj Viruses** to allow editorial control of the journal, including peer review and author/reviewer/editorial board management.
- To enable the use of personal data (subscriber, peer review, TOC alerts related) in reports to assist day-to-day management of the journal as well providing KPIs.

- To enable the sending of TOC alerts notifying Organisation members and further registrants of the latest journal issue release.

- To enable delivery of issues of the journal to customers and Organisation members, if applicable.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- For the duration of the contract

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- N/A

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 17

- Federal Republic of Germany

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Level of impact *Low = Category 1*
Medium = Category 1 + 2
High = Category 1 + Category 2 + Category 3

☒ Measures Category 1

☒ Measures Category 2

☐ Measures Category 3

*Low level of impact: Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.). Systems that fall into this category include: CRM/marketing tools that contain a small number of contacts (less than 1000) and do not contain attributes (profiles).

**Medium level of impact: Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.) OR a high number of individuals may be impacted. Systems that fall into this category include: E-learning systems, HR systems, CRM systems that contain a large number of contacts OR contain attributes (profiles).

***High/very high level of impact: Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.). Systems that fall into this category include: systems that contain health data such as medical examination results.

Category No.	**Measure Category**	**Measure Description**
Category 1 (Measures for Low, Medium and High Risk Level)		
1	Security policy and procedures for the protection of personal data	The Data Importer should document its policy with regards to personal data processing as part of its information security policy.

1	Security policy and procedures for the protection of personal data	The security policy should be reviewed and revised, if necessary, on an annual basis.
1	Roles and responsibilities	Roles and responsibilities related to the processing of personal data should be clearly defined and implemented following the need to know principle.
1	Roles and responsibilities	During internal reorganization or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.
1	Resource/asset management	The Data Importer should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).
1	Resource/asset management	IT resources should be reviewed and updated on regular basis.
1	Change management	The Data Importer should make sure that all changes to the IT system are logged. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
1	Change management	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.
1	Data processors	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.
1	Data processors	Formal requirements and obligations should be formally agreed between the data controller and the data Processor reflecting the requirements following this document. The data processor should provide sufficient documented evidence of compliance.
1	Incidents handling / Personal data breaches	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.

1	Business continuity	The Data Importer should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).
1	Confidentiality of personnel	The Data Importer should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.
1	Training	The Data Importer should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.
1	Access control and authentication	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.
1	Access control and authentication	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.
1	Access control and authentication	An authentication mechanism should be in place, allowing access to the IT System. As a minimum a username/password combination should be used. Password protection should meet current best practice.
1	Access control and authentication	User passwords must be stored in a “hashed” and salted form.
1	Access control and authentication	The access control system should have the ability to detect and not allow the usage of passwords that don’t respect the current best practice.
1	Logging and monitoring	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion). This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.

1	Logging and monitoring	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
1	Server/Database security	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
1	Server/Database security	For multi-tenant systems include functionality to separate personal Data from that of other Data Controllers. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
1	Workstation security	Users should not be able to deactivate or bypass security settings.
1	Workstation security	Anti-virus applications and detection signatures should be configured / deployed within 24 hours of being supplied by Vendors.
1	Workstation security	Users should not have privileges to install or deactivate unauthorized software applications.
1	Workstation security	The system should have session time outs when the user has not been active for a certain time period.
1	Workstation security	Critical security updates released by the operating system developer should be installed regularly.
1	Network/Communication security	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).
1	Back-ups	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.

1	Back-ups	To the extent backups are made, these backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.
1	Back-ups	Execution of backups should be monitored to ensure completeness. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
1	Back-ups	Full backups should be carried out regularly. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
1	Mobile/Portable devices	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.
1	Mobile/Portable devices	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.
1	Mobile/Portable devices	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.
1	Application lifecycle security	During the development lifecycle best practices, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.
1	Application lifecycle security	Specific security requirements should be defined during the early stages of the development lifecycle.
1	Application lifecycle security	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.
1	Application lifecycle security	Secure coding standards and practices should be followed.
1	Application lifecycle security	During the development, testing and validation against the implementation of the initial security requirements should be performed.
1	Data deletion/disposal	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed. To the

		extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
1	Data deletion/disposal	Shredding of paper and portable media used to store personal data shall be carried out. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
1	Physical security	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.
Category 2 (Measures for Medium and High Risk Level)		
2	Security policy and procedures for protection of personal data	The Data Importer should document a separate dedicated security policy with regard to the processing of personal data.
2	Security policy and procedures for protection of personal data	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisational measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.
2	Roles and responsibilities	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.
2	Access control policy	An access control policy should be detailed and documented. The Data Importer should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.
2	Access control policy	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.
2	Resource/asset management	Roles having access to certain resources should be defined and documented.

2	Data processors	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.
2	Incidents handling / Personal data breaches	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.
2	Incidents handling / Personal data breaches	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.
2	Business continuity	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.
2	Business continuity	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.
2	Confidentiality of personnel	Prior to up taking their duties employees should be asked to review and agree on the security policy of the Data Importer and sign respective confidentiality and non-disclosure agreements.
2	Training	The Data Importer should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.
2	Access control and authentication	A specific password policy should be defined and documented.
2	Logging and monitoring	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
2	Logging and monitoring	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
2	Logging and monitoring	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.

		This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
2	Server/Database security	Encryption solutions should be considered on specific files or records through software or hardware implementation. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
2	Server/Database security	Encrypting storage drives should be considered. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
2	Server/Database security	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information
2	Network/Communication security	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.
2	Network/Communication security	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.
2	Back-ups	Backup media should be regularly tested to ensure that they can be relied upon for emergency use. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
2	Back-ups	Scheduled incremental backups should be carried out at least on a daily basis. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.
2	Back-ups	To the extent backups are made, copies of the backups should be securely stored in different locations.
2	Back-ups	In case a third party (other than Data Exporter and Data Importer) service for back up storage is used, the copy must be encrypted before being transmitted from the data controller. This measure does not apply to the extent Data Importer accesses Data Exporter systems when providing its service.

2	Mobile/Portable devices	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.
2	Mobile/Portable devices	The Data Importer should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.
2	Mobile/Portable devices	Mobile devices should support separation of private and business use of the device through secure software containers.
2	Application lifecycle security	Vulnerability assessment, application and infrastructure penetration testing should be performed regularly. The application shall not be adopted unless the required level of security is achieved.
2	Application lifecycle security	Software patches should be tested and evaluated before they are installed in an operational environment.
2	Data deletion/disposal	Multiple passes of software-based overwriting should be performed on all media before being disposed. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
2	Data deletion/disposal	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate. To the extent Data Importer accesses Data Exporter systems when providing its service this measure only applies to the extent that Data Importer stores Data Exporter Data on its own systems.
2	Physical security	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the Data Importer's or its subcontractors' Data Importer should be established, as appropriate.
2	Physical security	At the Data Importer's and its subcontractors' premises, secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored.
2	Physical security	At the Data Importer's and its subcontractors' premises, intruder detection systems should be installed in all security zones.

2	Physical security	At the Data Importer's and its subcontractors' premises, physical barriers should, where applicable, be built to prevent unauthorized physical access.
2	Physical security	At the Data Importer's and its subcontractors' premises, vacant secure areas should be physically locked and periodically reviewed
2	Physical security	At the Data Importer's and its subcontractors' premises, an automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room
2	Physical security	At the Data Importer's and its subcontractors' premises, external party support service personnel should be granted restricted access to secure areas.

ANNEX III

TRANSFER IMPACT ASSESSMENT PURSUANT TO CLAUSE 14 OF THE STANDARD CONTRACTUAL CLAUSES (MODULE ONE, Controller-to-Controller-transfers)

Pursuant to Clause 14(b), the Parties undertake to use the following questionnaire to collect the relevant information as basis for the Transfer Impact Assessment:

- *Springer Nature TIA Questionnaire*

The Parties' warranty in accordance with Clause 14(a) is based on the information provided by the data importer through the aforementioned questionnaire, as incorporated in ANNEX IV.

ANNEX IV

TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE

Name and address of Data importer(s):	World Society for Virology 1 Envelope Terrace, Unit 115, Worcester, MA 01604, USA
Name/description of the transfer:	The purpose(s) of the data transfer and further processing is: To provide peer review data to the Editors of the journal **npj Viruses** to allow editorial control of the journal, including peer review and author/reviewer/editorial board management. To enable the use of personal data (subscriber, peer review, TOC alerts related) in reports to assist day-to-day management of the journal as well providing KPIs. To enable the sending of TOC alerts notifying Organisation members and further registrants of the latest journal issue release. To enable delivery of issues of the journal to customers and Organisation members, if applicable.

Part 1: Specific circumstances of the transfer (Cl. 14(b)(i) of the SCC)			
No.	**Questions**	**Options**	**Answer**
1	**Do you process personal data in your capacity as data controller (i.e. independently on your own behalf for your own purposes) or data processor (i.e. on our behalf, based on our instructions)?**	**Data controller**	Yes
		Data processor	No
2	**Which types of data do you process? Please select all that apply.**	**Name**	Yes

		Contact details (e.g. postal address, email address, phone number)	Yes
		IP address	No
		Data about the use of a service (e.g. times of use, frequency of use)	No
		Device data (e.g. operating system, browser version, screen resolution)	No
		Payment/billing data	No
		Location data	No
		Others (if yes, please comment):	No
3	**Does the processing involve information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning an individual's sex life or sexual orientation?**		No
4	**Which types of individuals are affected by the processing, i.e. whose data do you process? Please select all that apply.**	**Our employees**	No
		Our users/customers	Yes
		Our suppliers/contractors/ business partners	No
		Others (if yes, please comment):	No

5	**Do you share personal data received from us with other data recipients (e.g. service providers, other group companies etc.)?**	**To other data controller(s)**	No
		To other data processor(s)	No
6	**Where do these other data recipients (e.g. service providers, other group companies etc.) process the data, including locations of remote access to the personal data?**	**Within the EEA**	N/A
		In countries with EU Commission adequacy decision	N/A
		Outside the EEA	N/A
7	**What measures (i.e. legal transfer mechanism) are currently implemented to safeguard the transfer from you to your data recipients, i.e. to ensure a secure and legal transfer?**	**Binding Corporate Rules**	N/A
		EU Standard Contractual Clauses	Yes
		Consent	N/A

Part 2: Laws and practices of the third country you process personal data in (Cl. 14(b)(ii) of the SCC)		
No.	**Questions**	**Answer**
1	**Are you or any recipients with whom you share the personal data received from us subject to legal or factual obligations of the third country requiring the disclosure of data to public authorities or authorizing access by such authorities, relevant in light of the specific circumstances of the transfer?**	**No**
2	**Only if you are located in the US:**	

	Are you subject to national laws that allow public authorities access to personal data transferred from the EU (particularly 50 U.S.C. § 1881a (= FISA 702))?	Yes
	Are any recipients with whom you share the personal data received from us subject to national laws that allow public authorities access to personal data transferred from the EU (particularly 50 U.S.C. § 1881a (= FISA 702))?	N/A
If you answered "No", on question 1 and 2 of Part 2, please continue with Part 3. If you answered "Yes" on question 1 or 2 of Part 2, please continue with question 3.		
3	**Do you or the recipients with whom you share personal data received from us have to proactively transmit personal data to authorities (particularly in the US) in certain cases?**	No
4	**Does the law and/or government policy require you to create back doors to facilitate public authority access or create/change business processes to facilitate access and/or have you created such back doors?**	No
5	**In a case where authorities (particularly in the US) are entitled to access personal data transferred from the EU or where you or the recipients with whom you share personal data received from us are obliged to proactively transfer such data: are you or the recipients with whom you share the personal data received from us allowed to inform us as data exporter and/or the data subject about the access of the authorities to the personal data from the EU?**	Yes
6	**Are there any legal remedies for you and/or the data subjects concerning the access to personal data by public authorities?**	Yes
7	**Do you have relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests? Particularly:**	No
7a	**Have you or the recipients with whom you share personal data received from us submitted or disclosed personal data processed on behalf of a customer to an authority within the last 12 months?**	No

7b	**If yes, were you able to successfully fend off some/all of the requests?**	N/A
8	**Do you have internal records or other documentation drawn up on a continuous basis in accordance with due diligence and certified at senior management level on access requests (including the response provided and the reasoning)?**	Yes
9	**Do you publish regular reports on public authority access (including information on the number of requests received, measures taken, response provided)?**	No
10	**Is there any publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector you are in and/or the application of the law in practice, such as case law and reports by independent oversight bodies?**	Yes

Part 3: Relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the SCC (Cl. 14(b)(iii) of the SCC)			
No.	**Questions**	**Options**	**Answer**
1	**Do you need access to the data in unencrypted (i.e. as "clear" data) form?**		Yes
2	**Do you encrypt the data?**	**Data encryption at rest**	No
		Data encryption in transit	Yes
		No, economically not feasible	N/A
		No, technically not feasible	N/A

2a	**If yes: (i) Does the encryption you use conform to the state-of-the-art, (ii) can the encryption be considered robust against cryptanalysis performed by the public authorities in your country and (iii) is it flawlessly implemented by properly maintained software?** **(if "no", please provide a reason, e.g. technically not feasible)**		Yes
2b	**If yes: Who has control over the encryption key?**	**Data exporter (we=SN entity)**	Yes
		Data importer (you)	Yes
3	**Do you exclusively process pseudonymized data (i.e. data that may not immediately be linked to an individual e.g. because names are replaced with customer IDs)?**		No
4	**If yes: Can you de-pseudonymize the data without our help, i.e. can you reconstruct a personal reference from the "abstract" data without our help, so that you know to which individual the data belong?**		N/A

Certificate Of Completion

Envelope Id: 89FBBDE5-F162-42A6-B5E8-63DCBB94D6E0
Status: Completed
Subject: Please review and sign these documents
Source Envelope:
Document Pages: 36
Signatures: 6
Certificate Pages: 2
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Envelope Originator:
Nicolas Fanget
MRPA/IT Procurement 0950
Heidelberger Platz 3
Berlin, Germany 14197
n.fanget@nature.com
IP Address: 51.124.79.122

Record Tracking

Status: Original
1/6/2026 3:59:28 PM
Holder: Nicolas Fanget
n.fanget@nature.com
Location: DocuSign

Signer Events	Signature	Timestamp
Joe Bennett j.bennett@nature.com Mr Springer Nature Security Level: Email, Account Authentication (None)	DocuSigned by: Joe Bennett 4F1C9BDAC1FC43B... Signature Adoption: Pre-selected Style Using IP Address: 170.85.58.82	Sent: 1/6/2026 4:02:04 PM Viewed: 1/8/2026 2:30:11 PM Signed: 1/8/2026 2:31:52 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Prof. Maria Söderlund-Venermo maria.soderlund-venermo@helsinki.fi Security Level: Email, Account Authentication (None)	Signed by: Prof. Maria Söderlund-Venermo 06A72E0591CD491... Signature Adoption: Pre-selected Style Using IP Address: 85.76.100.227	Sent: 1/6/2026 4:02:03 PM Viewed: 1/7/2026 7:29:34 AM Signed: 1/8/2026 12:19:14 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Prof. Marietjie Venter marietjie.venter1@wits.ac.za Security Level: Email, Account Authentication (None)	Signed by: Prof. Marietjie Venter E122E5C03A9A410... Signature Adoption: Pre-selected Style Using IP Address: 169.0.82.50 Signed using mobile	Sent: 1/6/2026 4:02:03 PM Viewed: 1/12/2026 10:43:00 PM Signed: 1/12/2026 10:45:50 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Scott Rae scott.rae@nature.com Springer Nature Security Level: Email, Account Authentication (None)	Signed by: Scott Rae 41D7D48AB3B44DD... Signature Adoption: Pre-selected Style Using IP Address: 170.85.58.115	Sent: 1/6/2026 4:02:03 PM Viewed: 1/6/2026 4:15:46 PM Signed: 1/6/2026 4:15:50 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	1/6/2026 4:02:04 PM
Certified Delivered	Security Checked	1/6/2026 4:15:46 PM
Signing Complete	Security Checked	1/6/2026 4:15:50 PM
Completed	Security Checked	1/12/2026 10:45:50 PM

Payment Events	Status	Timestamps