ePrivacyseal

C E R T I F I C A T E

no. 470/23

ePrivacyseal GmbH
Burchardstr. 14, 20095 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 13 December 2023

BGI EUROPE A/S
Symfonivej 34, 2730 Herlev, Denmark

sells its product or service
„HALOS Appliance“
version V4
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate.

final audit day: 12/12/2023
next planned monitoring by 11/12/2026
period of validity: 12/12/2023 – 11/12/2026

The certification decision takes place under the validity condition described in Annex 3
and in conformity with the criteria catalogue for the “ePrivacyseal EU” (version 3.0 of May 2022)
of ePrivacyseal GmbH.

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

Annex 1 to certificate no. 470/23

Definition of processing activities

HALOS Appliance from BGI provides customers with a platform for bioinformatics analysis. It is intended for internal use in hospitals or laboratories.

HALOS Appliance is an integrated system platform with hardware and software, consisting of server and terminal PC, used for bioinformatics analysis and related data management. It also provides an interface to the sequencer to obtain FASTQ files. The product is designed for internal use in hospitals and allows hospital staff to enter relevant information such as samples and analysis tasks. Then, HALOS Appliance can retrieve off-board data from the sequencer, analyze it automatically, and finally generate test reports. HALOS Appliance can be deployed in local IT centers or sequencing experiment centers to provide in-house bioinformatics analysis services to medical facilities and scientific research institutes.

Annex 2 to certificate no. 470/23

Excluded processing activities

The following functions and/or services and/or product-versions are not subject to this evaluation and have not been reviewed by the experts:

- Hardware (this also includes, for example, the sequencer)
- Processing activities requiring internet connection or data transfer to the internet
- Data processing in third countries (third country transfer)
- Third party applications
- Services of third parties, which are not named in “Third Parties” table
- Third party systems such as Operating System (Microsoft Windows)
- System logging: Any logging not specified in the process is out of scope.
- Backups: Only the server database backup process in the management center is in scope as described in the technical facutal description. All other backups are out of scope. Once the backup leaves HALOS Appliance, it is out of scope.
- Any algorithm that is considered to be AI

Annex 3 to certificate no. 470/23

Validity condition

The seal is awarded on the following validity conditions:

1. To ensure data security in accordance with the GDPR, the controller must use self-signed certificates. Compliance is not possible without self-signed certificates.
2. The encryption with AES 256 must not be changed or switched off.
3. The hashing of the login password with SHA 256 is not allowed to be changed or switched off.
4. The seal is only valid if the company using HALOS has sufficient technical and organisational measures.
5. Only the data types listed in "Data Types" sheet must be processed.
6. The data is not transferred to or accessed from countries outside the EU/EEA (third countries).
7. On condition that the FASTQ file is encrypted with AES256 or better.

Further Validity Conditions derive from the Certification Criteria, due to the fact that the subject of certification is an IT product, not a processing activity:

Referring to chapter I, "General Principles":

8. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance adheres to the Terms of Use and the Data Protection Policy for HALOS Appliance, and therefore abides to the principles of Art. 5 General Data Protection Regulation ("GDPR") as far as they are implemented in HALOS Appliance, the principles for processing personal data pursuant to Art. 5 GDPR will be observed (referring to Chapter I, **No. 3.1 – 3.14** of *Certification Criteria*).
9. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the roles and permissions model according to the user's classification, then the aspect of limit the use of data to the necessary extent of the principle of data minimization will be met (referring to Chapter I, **No. 3.3** of *Certification Criteria*).
10. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the integrated function to delete data that is no longer necessary for the purposes intended with HALOS Appliance, it can be ensured that the personal data are not stored for longer than necessary and, therefore, meets the principle of storage limitation (referring to Chapter I, **No. 3.5** of *Certification Criteria*).
11. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance has a complete, valid deletion concept in place that ensures that all data is deleted according to the applicable requirements, especially according to GDPR, the principle of storage limitation is met (referring to Chapter I, **No. 3.5** of *Certification Criteria*). Especially, the deletion concept must ensure that storage periods are selected in such a way that the data is not stored for longer than is permitted under data protection law and its processing is necessary.
12. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the permission authentication and access control mechanism provided by HALOS Appliance, personal data will be processed in a manner that ensures adequate

security of the personal data in a way that the requirements for integrity and confidentiality are met (referring to Chapter I, **No. 3.6** of *Certification Criteria*).

13. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the function to delete all personal data that is no longer necessarily for the purpose intended, the principle of data minimization and storage limitation can be met (referring to Chapter I, **No. 3.10** of *Certification Criteria*).
14. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance abides by the provided detailed guidance how to document compliance with data protection principles in the Data Protection Guidance for Customers, the principle of accountability can be met (referring to Chapter I, **No. 3.14** of *Certification Criteria*).
15. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance abides by the purposes of data processing the product may be used for as described in the Privacy and Security Handbook (No. 2.5.1, for non-genomic data, and No. 2.5.2 for genomic data), the purpose for which the data is to be collected and processed has already been specified when the data is collected (referring to Chapter I, **No. 5.1** of *Certification Criteria*) and it is documented accordingly (referring to Chapter I, **No. 5.2** of *Certification Criteria*), and, therefore, the purpose limitation principle is fulfilled.
16. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance stores data of different origins (like samples of different patients) in HALOS Appliance in a way that the individual data can only be read out for a specific purpose of data sequencing, the requirements for the separation of data are met (referring to Chapter I, **No. 6.2** of *Certification Criteria*).

Referring to chapter II, "Lawfulness of the Processing":

17. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance provides guidance to its employees as established in the HALOS Appliance "Data Protection Guidance for Customers" on how to examine the legal basis and has internal clear structures and responsibilities to determine the legal basis, the controller's obligation to provide sufficient help to determine the structures for checking a sufficient legal basis are met (referring to Chapter II, **No. 1.0** of *Certification Criteria*).
18. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance and the legal basis for the processing subsequently ceases to exist and the controller deletes the data unless there is a legal exception, the controller meets the requirements for a valid legal basis (referring to Chapter II, **No. 1.0** of *Certification Criteria*).
19. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance processes the personal data of the patients based on one of the legal bases of Art. 6 para. 1 GDPR or Art. 9 para. 2 GDPR – if applicable – and fulfills the specific requirements of each basis, e.g. using the applicant's Sample consent Form, the lawfulness of the processing is given (referring to Chapter II, **No. 1.1-1.6.3** of *Certification Criteria*).
20. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance processes personal data for other purposes than for which the data have

been collected and the processing is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives – which is regarded to be irrelevant in the case at hand – takes into account all relevant aspects in Art. 6 para. 4 GDPR to ascertain that the new purpose is compatible with the original purpose (referring to Chapter II, **No. 1.7** of *Certification Criteria*), the requirements for a change of purpose are met.

21. Under the assumption that the controller carrying out data processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR with HALOS Appliance by fulfilling one of the exceptional circumstances listed in Art. 9 para. 2 GDPR, the processing is lawful (referring to Chapter II, **No. 2.2.1-2.2.10** of *Certification Criteria*).

Referring to chapter III, "Guarantee of data subject rights, Art. 12 et seq. GDPR":

22. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses e.g. the sample "Data Protection Notice" provided by the applicant, and completes the provided sample according to the actual circumstances and in compliance Art. 13 GDPR or uses a different information meeting the requirements in Art. 12, 13 GDPR for the cases described in Art. 13 para. 1 GDPR, the information requirements can be met (referring to Chapter III, **No. 1.1-1.4** of *Certification Criteria*).
23. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance intends to further process personal data for a purpose other than for which the personal data were collected and in case the data subject does not already have information on the processing, and the controller provides the data subject prior to that further processing with information on that other purpose and with the relevant further information as referred to in Art. 13 para. 2 GDPR, the information requirements when changing the legal basis are met (referring to Chapter III, **No. 1.4** of *Certification Criteria*).
24. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance creates a "Data Protection Notice" for the cases described in Art. 14 paras. 1, 2, 3 GDPR and the document created meets the requirements set forth in the respective rules, the information requirement of Art. 14 GDPR is met (referring to Chapter III, **No. 1.5.1-1.5.14** of *Certification Criteria*).
25. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance intends to process the data for a purpose other than for which the personal data were obtained, and the controller provides information on that new purpose as referred to in Art. 14 para. 4 GDPR, the controller meets the information requirements (referring to Chapter III, **No. 1.5.15** of *Certification Criteria*).
26. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance confirms upon request the processing of personal data and gives access to the information pursuant to Art. 15 para. 1 lit. (a) – (h), para. 2 – if applicable – in a technically available way for the data subject within an acceptable timeframe and offers the first copy – as long as the copy does not affect the rights and freedoms of others - of the data free of charge, the requirements for the right of access are met (referring to Chapter III, **No.**

2 of *Certification Criteria*).

27. Under the assumption that a modification of genomic data is not possible due to the nature of the data and under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the function to modify non-genomic data and/or account information free of charge through the functions Edit/Delete Customer Information and Edit, Delete User function, the requirements to comply with the right to rectification according to Art. 16 GDPR are met (referring to Chapter III, **No. 3** of *Certification Criteria*).
28. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance erases and/or blocks personal data without undue delay, provided that one of the reasons of Art. 17 para. 1 GDPR applies and the processing is not necessary pursuant to Art. 17 para. 3 GDPR and it is ensured that the personal data is deleted completely and irreversibly, at the legally binding time in each case and cannot be recovered in case of a deletion, the right to erasure or blocking of personal data is met (referring to Chapter III, **No. 4** of *Certification Criteria*).
29. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance restricts the processing in cases of Art. 18 para. 1 GDPR and informs the data subject about the successful restriction, the right to restriction of processing is met as long as the controller operates the data just in cases of Art 18 para. 2 GDPR (referring to Chapter III, **No. 5** of *Certification Criteria*).
30. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance uses the HALOS Appliance to export the personal data requested by the data subject to his/her local data center or to other local storage devices in a readable or data subject required format (e.g. .fastq) and to deliver it to the data subject or another controller, in a way pursuant to Art. 20 GDPR, the right to data portability is fulfilled (referring to Chapter III, **No. 6** of *Certification Criteria*).
31. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance processes data on the basis on Art. 6 para. 1 lit. f) GDPR and the data subject uses his or her right to object the processing and the data controller quits processing, prerequisites of Art. 21 GDPR can be met (referring to Chapter III, **No. 7** of *Certification Criteria*).
32. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance communicates any rectification or erasure of personal data or restriction of processing to each recipient of the data free of charge and informs the data subject on demand about those recipients, the controller meets the obligation to forward and to inform to a potential second controller that actually stored the data (referring to Chapter III, **No. 9** of *Certification Criteria*).

Referring to chapter IV, "Data protection management"

33. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance maintains a register of all processing activities under its responsibility containing information pursuant to Art. 30 para. 1 GDPR in writing or in an electronic format

and the controller has established processes to keep the register up-to-date and created it by including all the relevant departments, a sufficient record of processing activities is created (referring to Chapter IV, **No. 1** of *Certification Criteria*).

34. Under the assumption that the processing of personal data with HALOS Appliance is carried out by a processor that provided sufficient technical and organizational measures and with whom a data processing agreement as defined in Art. 28 para. 1, 3 GDPR exists and the processor does not use the services of other processors without the prior separate or general written consent of the controller, therefore, the legal requirements to include a third party in the processing are met (referring to Chapter IV, **No. 2** of *Certification Criteria*).
35. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance will perform a threshold analysis and a DPIA, if necessary, that covers the minimum requirements defined in the GDPR, the prerequisites of Art. 35 para. 1 GDPR will be observed (referring to Chapter IV, **No. 8** of *Certification Criteria*) and the requirements met.
36. Under the assumption that the controller carrying out data processing of personal data with HALOS Appliance is obliged to appoint a Data Protection Officer (DPO) and the DPO is sufficiently qualified and fulfills his duties according to Art. 39 GDPR lawfully, the requirements of Art. 37 ff. GDPR are met (referring to Chapter IV, **No. 9** of *Certification Criteria*).