Discoverer Data Processing Agreement (DPA)

Article 28 data processing terms for personal data on Discoverer

Version 1.0 · 8 June 2026

Related documents:

- Discoverer Access Policy
- Discoverer Acceptable Use Policy (AUP)
- Discoverer Use Policy (DUP)

Veselin Kolev
v.kolev@discoverer.bg

Discoverer Petascale supercomputer
Sofia Tech Park, Sofia, Bulgaria
https://discoverer.bg
https://docs.discoverer.bg

Contents

Preface

Scope of the document

This Data Processing Agreement (DPA) sets out the contractual terms under which PetaSC processes personal data on behalf of a Customer when that data is stored or processed on the Discoverer petascale supercomputer at SofiaTech Park, Sofia, Bulgaria. The infrastructure comprises two clusters: Discoverer (CPU cluster) and Discoverer+ (GPU cluster), together with associated storage and access services described in the Discoverer Use Policy (DUP).

PetaSC is the consortium that operates the Discoverer petascale supercomputer — both the Discoverer CPU cluster and the Discoverer+ GPU cluster — including shared storage, identity and access systems, scheduling, and user support.

This DPA implements Article 28 of Regulation (EU) 2016/679 (GDPR) where PetaSC acts as processor for Customer Personal Data. It does not replace the Acceptable Use Policy (AUP) or the DUP, which remain binding on all End Users.

Relationship to other policies

This agreement complements

- the Discoverer Access Policy, which governs how access time is allocated;
- the Acceptable Use Policy (AUP), which governs lawful and ethical conduct, including high-level data-protection rules in AUP §8; and
- the Discoverer Use Policy (DUP), which governs operational and technical rules for accounts, storage, retention, and monitoring.

Account personal data used to provision LDAP/POSIX identities (Given Name, Family Name, e-mail address) are described in DUP §3.6 and AUP §8.1. PetaSC processes those data primarily to operate access to Discoverer and is independent controller for that operational processing unless mandatory law or a separate written agreement states otherwise. Customer Personal Data placed in project workloads is in scope of this DPA.

In case of conflict between this DPA and a project-specific commercial contract that explicitly addresses data protection, the commercial contract prevails for that Customer. Otherwise, the order of precedence for data protection matters shall be: this DPA (where signed), the AUP, the DUP, and operational documentation at https://docs.discoverer.bg, unless mandatory law provides otherwise.

1. Introduction

1.1 Purpose

This DPA ensures that when a Customer uses Discoverer to store or process personal data relating to identifiable individuals, PetaSC processes that data only on documented instructions, with appropriate security measures, and in compliance with applicable data-protection law.

1.2 Parties

This agreement is entered into between

- PetaSC, as processor, operating the Discoverer service at SofiaTech Park, Sofia, Bulgaria; and
- the Customer, as controller, being the legal entity named in the signature block (§20) — typically the PI's home institution, research organisation, or commercial company that holds the allocation or contract for the project identified in Annex A.

End Users act under the Customer's authority. Individual End Users do not sign this DPA unless they are the Customer in their own right (for example a sole trader with a direct commercial contract).

2. Scope and applicability

2.1 When this DPA applies

This DPA applies when all of the following are true

- the Customer has an active allocation, commercial contract, or other authorised access to Discoverer or Discoverer+;
- the Customer instructs PetaSC — through normal use of the platform under the AUP and DUP — to store or process Customer Personal Data on Discoverer storage or compute resources; and
- the Customer and PetaSC have executed the signature blocks in §20, or the DPA is incorporated by reference in a signed commercial contract or award letter.

Projects that process only non-personal scientific or technical data do not require a separate DPA signature, but remain subject to the AUP and DUP.

2.2 When this DPA does not replace other arrangements

EuroHPC or national allocations where the Customer's institution already holds a framework agreement with PetaSC or its host partners may satisfy Article 28 requirements through that framework. Where such an agreement exists and explicitly covers Discoverer processing, it prevails over this template for that institution. Otherwise, PetaSC may require execution of this DPA before personal data are placed in project storage.

2.3 Covered systems

This DPA covers processing on systems operated by PetaSC for the Customer's project, including login nodes, compute nodes, project and home storage, SLURM accounting records that reference project and user identifiers, LDAP directory entries used to administer access, VPN and SSH access logs, backup copies of stored data, and support tickets relating to the project. A detailed system list appears in Annex A.

3. Definitions

For the purposes of this agreement

- Customer — the controller named in §20 that determines the purposes and means of processing Customer Personal Data on Discoverer.
- Customer Personal Data — personal data contained in datasets, job inputs or outputs, software configurations, or other files that the Customer or its End Users store or process on Discoverer under the approved project or contract, and that PetaSC processes on the Customer's documented instructions through provision of the service.
- Data protection legislation — Regulation (EU) 2016/679 (GDPR) and applicable national implementing law, including the Bulgarian Personal Data Protection Act where it applies.
- Discoverer — the CPU cluster of the Discoverer supercomputing service, including login nodes and CPU compute partitions.
- Discoverer+ — the GPU cluster of the service, including login nodes and GPU compute partitions.
- DPA — this Data Processing Agreement.
- End User — any person granted an LDAP/POSIX account and authorised to access one or both clusters under the Customer's project, as defined in the AUP.
- Personal data, processing, controller, processor, data subject, and personal data breach — as defined in the GDPR.
- PetaSC — the consortium that operates the Discoverer petascale supercomputer at SofiaTech Park, comprising the Discoverer (CPU) cluster and the Discoverer+ (GPU) cluster, together with shared storage, identity and access systems, scheduling, and user support.
- Principal Investigator (PI) — the person responsible for the project allocation, as defined in the Access Policy, acting on behalf of the Customer unless the Customer is identified separately in the contract.
- Sub-processor — any third party engaged by PetaSC to process Customer Personal Data on PetaSC's behalf.
- Supervisory authority — an independent public authority established under Article 51 GDPR.

Other capitalised terms align with the Access Policy, AUP, and DUP.

4. Roles and processing activities

4.1 Processor role of PetaSC

For Customer Personal Data stored or processed in project workloads, PetaSC acts as processor. PetaSC shall process Customer Personal Data only on documented instructions from the Customer, except where required by Union or Member State law.

4.2 Controller role of the Customer

The Customer is controller for Customer Personal Data. The Customer is responsible for:

- establishing a lawful basis for processing under the GDPR;
- providing privacy information to data subjects;
- ensuring that End Users process data only within the approved project scope (AUP §8.1);
- ensuring that export-controlled, special-category, or otherwise restricted data are not transferred to Discoverer without appropriate safeguards and prior agreement with PetaSC where needed.

4.3 Operational account data

PetaSC processes End User account data (Given Name, Family Name, e-mail address, POSIX username, SSH public keys, group memberships, SLURM account associations) to provision and operate access. That processing supports both the Customer's project and the shared platform. Data subject requests relating to account data should be directed to PetaSC under AUP §8.1 and §13.

4.4 End Users

End Users are not parties to this DPA. They accept the AUP (§14.3) and must comply with the Customer's instructions and applicable law when handling Customer Personal Data on Discoverer.

5. Subject matter, duration, nature, and purpose

5.1 Subject matter

Provision of high-performance computing, storage, and related support services on Discoverer and Discoverer+ for the project identified in Annex A.

5.2 Duration

From the date of the last signature in §20 until Customer Personal Data have been deleted or returned in accordance with §14 and DUP §8.4–§8.5, and any agreed extended retention under DUP §8.6 has ended.

5.3 Nature of processing

Storage, execution of batch and interactive jobs, backup, replication within the PetaSC facility where configured, data transfer via documented endpoints, access control through LDAP and POSIX permissions, SLURM scheduling and accounting, operational and security monitoring, and deletion at end of retention.

5.4 Purpose of processing

To enable the Customer and its End Users to conduct approved research, development, or commercial workloads on shared infrastructure, and to allow PetaSC to operate, secure, and account for use of that infrastructure.

6. Types of personal data and categories of data subjects

6.1 Customer declaration

The Customer shall describe the categories of Customer Personal Data and data subjects in Annex A before substantial personal-data processing begins. Typical categories include:

Customer Personal Data types (examples)

- identifiers (names, internal IDs, patient or participant codes if pseudonymised);
- contact details when present in research datasets;
- health or biometric data where the Customer's lawful research requires it;
- any other categories the Customer uploads to project or home storage.

Categories of data subjects (examples)

- research participants;
- patients or donors in biomedical studies;
- employees or contractors of the Customer;
- other individuals whose data the Customer lawfully processes for the project.

The Customer shall not upload special-category data unless it has established an appropriate lawful basis and, where required, has notified PetaSC so that additional safeguards can be agreed.

6.2 Metadata processed by PetaSC

In operating the service, PetaSC also processes metadata that may relate to identifiable End Users (for example POSIX username, project account name, job identifiers, IP addresses in logs, and support correspondence). Such metadata is processed to deliver the service and is described in Annex A.

7. Controller obligations and documented instructions

7.1 Documented instructions

The Customer instructs PetaSC to process Customer Personal Data by

- storing and running workloads within the project scope approved in the allocation or contract;
- managing project rosters through PetaSC as described in DUP §3.7;
- using Discoverer only in accordance with the AUP, DUP, and operational documentation;
- requesting agreed extended retention or secure export before retention deadlines in DUP §8.4–§8.5.

Instructions outside this scope require prior written agreement. PetaSC shall inform the Customer if it believes an instruction infringes the GDPR or other applicable data-protection law.

7.2 Customer warranties

The Customer warrants that

- it has a valid legal basis for all Customer Personal Data processed on Discoverer;
- data subjects have received required information, or the Customer will provide it without undue delay;
- End Users are bound by confidentiality and data-protection obligations adequate for the processing;
- transfer of Customer Personal Data to Discoverer complies with applicable transfer rules (§13).

7.3 End User roster

The PI shall keep the project roster accurate and notify PetaSC when End Users leave, so access and retention rules apply correctly (DUP §3.7, §8.5).

8. Processor obligations

PetaSC shall

- process Customer Personal Data only on documented instructions from the Customer, unless required by law — in which case PetaSC shall inform the Customer of that legal requirement before processing where permitted;
- ensure that persons authorised to process Customer Personal Data are bound by confidentiality;
- implement appropriate technical and organisational measures under §10 and Annex B;
- respect the conditions for engaging Sub-processors under §9;
- taking into account the nature of processing, assist the Customer with data subject rights requests under §12;
- assist the Customer with security, breach notification, and data-protection impact assessment obligations where reasonable and considering the nature of processing;
- at the Customer's choice, delete or return Customer Personal Data after the end of provision of services relating to processing, subject to §14 and mandatory retention law;
- make available information necessary to demonstrate compliance and allow audits under §16;
- inform the Customer without undue delay if PetaSC becomes aware of a personal data breach affecting Customer Personal Data.

PetaSC does not routinely inspect the content of Customer Personal Data in project datasets (AUP §8.1). Inspection may occur where required by law, contractual audit rights, or a substantiated security concern (AUP §8.1, §11.3; DUP §7.6).

9. Sub-processors

9.1 Authorised Sub-processors

The Customer grants PetaSC general written authorisation to engage Sub-processors that provide hosting, connectivity, backup, monitoring, or identity services necessary to operate Discoverer at SofiaTech Park, provided PetaSC imposes data-protection terms no less protective than this DPA.

PetaSC's primary processing and storage occur within the PetaSC facility in Bulgaria (AUP §8.4). Sub-processors outside the European Economic Area shall be used only with appropriate transfer safeguards under §13.

9.2 List and changes

PetaSC shall maintain a list of Sub-processors material to Customer Personal Data processing and publish updates on https://docs.discoverer.bg or provide them on request. PetaSC shall notify the Customer of intended changes giving reasonable notice so the Customer may object on substantiated data-protection grounds. If the parties cannot resolve an objection, the Customer may terminate processing of Customer Personal Data on Discoverer in accordance with §14.

9.3 Responsibility

PetaSC remains responsible to the Customer for the performance of Sub-processors' obligations.

10. Security of processing

PetaSC implements technical and organisational measures appropriate to the risks of processing, including those listed in Annex B. Measures include logical separation of projects through POSIX groups and project storage paths (DUP §3.7), access control through LDAP group membership and SSH key management (DUP §3.6, §11.1), network access controls including VPN requirements, monitoring for security and abuse (AUP §11, DUP §10.4, §14), and backup procedures described in the DUP.

The Customer is responsible for security measures within its control, including strong credentials hygiene, appropriate file permissions within project directories, encryption of sensitive datasets where required by the Customer's policy, and timely export of data before retention deadlines.

11. Personal data breaches

11.1 Notification to the Customer

PetaSC shall notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notification shall include, to the extent available:

- a description of the nature of the breach;
- categories and approximate number of data subjects and records concerned;
- likely consequences;
- measures taken or proposed to address the breach.

PetaSC shall provide further information as it becomes available.

11.2 Customer responsibilities

The Customer is responsible for notifying supervisory authorities and data subjects where required by the GDPR. PetaSC shall cooperate with reasonable requests for information needed for those notifications.

12. Data subject rights and assistance

12.1 Requests via the Customer

Data subjects should submit access, rectification, erasure, restriction, portability, and objection requests to the Customer as controller. PetaSC shall forward to the Customer any request received directly regarding Customer Personal Data in project datasets, unless mandatory law requires otherwise.

12.2 Account data requests

Requests relating to End User account personal data in the LDAP directory (Given Name, Family Name, e-mail) should be directed to PetaSC under AUP §8.1 and §13. PetaSC shall respond in accordance with applicable law and operational retention rules in DUP §3.6 and §8.

12.3 Assistance

PetaSC shall assist the Customer with fulfilment of data subject rights where technically feasible, considering the shared HPC environment and retention policies. Erasure of data embedded in shared backups or logs may be limited by operational necessity and legal retention; PetaSC shall explain constraints when they apply.

13. International transfers

Primary processing and storage of Customer Personal Data occur in Bulgaria within the PetaSC facility at SofiaTech Park (AUP §8.4).

If the Customer exports data from Discoverer to third countries, the Customer remains responsible for lawful transfer. If PetaSC uses a Sub-processor outside the European Economic Area, PetaSC shall ensure appropriate safeguards such as adequacy decisions, standard contractual clauses, or other mechanisms recognised under Chapter V GDPR.

14. Return and deletion of personal data

14.1 Customer export obligation

The Customer and its End Users shall export Customer Personal Data from project storage within 30 days after the project end date, and from home directories within 30 days after an End User no longer belongs to any valid project, as defined in DUP §8.4 and §8.5.

14.2 Deletion by PetaSC

After applicable retention periods, PetaSC deletes Customer Personal Data using standard filesystem deletion procedures (DUP §8.7). Backups and logs may retain fragments for a limited operational window consistent with Annex B; PetaSC shall not use retained fragments for unrelated purposes.

14.3 Return on request

Before deletion, the Customer may request a copy of Customer Personal Data in a standard format where technically feasible and within retention windows. Requests for extended retention must follow DUP §8.6.

15. Termination

Either party may terminate this DPA as it relates to future processing of Customer Personal Data by ending the underlying allocation or contract and ensuring export or deletion under §14. Termination does not affect obligations that by nature survive, including confidentiality, breach notification for past incidents, and audit rights for processing that occurred while the DPA was in force.

16. Audits and information

16.1 Information

PetaSC shall make available this DPA, Annex B, and relevant compliance information on request, subject to confidentiality and security.

16.2 Audits

The Customer may audit PetaSC's compliance with this DPA no more than once per calendar year, unless a personal data breach or supervisory authority requirement justifies additional audit. Audits shall be conducted during business hours with reasonable notice, without disrupting other customers' security, and under confidentiality terms. The Customer bears its own audit costs unless an audit reveals material non-compliance attributable to PetaSC.

PetaSC may satisfy audit requests through independent reports or certifications where available and appropriate to the processing.

17. Liability and governing law

17.1 Liability

Each party's liability under this DPA is subject to the limitation and indemnity provisions of the applicable allocation contract or Access Policy commercial terms, where present. If no such provisions apply, liability shall be governed by applicable mandatory law.

17.2 Governing law and jurisdiction

This DPA is governed by the laws of Bulgaria. Courts in Sofia, Bulgaria shall have jurisdiction unless mandatory consumer or public-sector rules provide otherwise.

18. Changes to this agreement

Material amendments require approval by the Discoverer Management Team (DMT) and chairman of PetaSC where they affect published processor obligations. Updated versions are published at https://docs.discoverer.bg/dpa.pdf. PetaSC shall notify active Customers with signed DPAs of substantive changes. Continued processing of Customer Personal Data after the effective date of an update constitutes acceptance unless the Customer terminates in accordance with §14.

19. Contact

General support and data-protection questions: contact details on https://discoverer.bg and Getting help.

Security incidents: report through the support channel with subject line indicating security urgency; escalation to the Operational Manager (OM).

Data protection requests relating to account personal data or processor assistance under this DPA: contact PetaSC using the same support channel (AUP §13).

20. Acceptance and signatures

This section applies to Customers that execute this DPA for a project allocated directly by PetaSC or where this DPA is not already incorporated in a signed commercial contract.

For EuroHPC portal allocations, the Customer's institution may accept this DPA through the portal workflow or a separate institutional signatory process defined in the award documentation. Where no separate signature is collected, End User obligations under the AUP (§14.3) still apply; the Customer remains controller for Customer Personal Data.

20.1 Customer (controller)

Legal name of organisation

Registered address

Project / SLURM account ID

Authorised signatory name and role

Signature

20.2 PetaSC (processor)

Name

Role (BDM or delegate)

Signature

20.3 Annex A completion

Project description and categories of Customer Personal Data (see §6.1)

Appendix A — Description of processing

Item	Detail
Project / SLURM account ID	(completed at signing)

(continued on next page)

Item	Detail
Customer organisation	(completed at signing)
Project summary	(completed at signing)
Categories of Customer Personal Data	(completed at signing)
Categories of data subjects	(completed at signing)
Primary storage paths	`/valhalla/projects/<account>/`, optional `/weka` project folders, End User `$HOME` on shared filesystems (DUP §7)
Compute resources	Discoverer (CPU) and/or Discoverer+ (GPU) partitions per allocation
Identity and access	LDAP/POSIX directory, SSH public keys, VPN where applicable (DUP §3.6, §11.1)
Scheduling and accounting	SLURM with project account and QoS (DUP §3.8, §4, §14)
Logs and monitoring	Login and job accounting logs, network monitoring for security (AUP §11, DUP §10.4, §14)
Support	Tickets and correspondence via PetaSC support channels
Backups	As described in DUP §8
Location	SofiaTech Park, Sofia, Bulgaria

Appendix B — Technical and organisational measures

Access control

- Unique LDAP/POSIX account per End User; cluster entitlement through group membership (DUP §3.6–§3.7).
- SSH public keys administered by PetaSC; password login not used for routine access (DUP §11.1).
- Project data isolated by POSIX group ownership on project directories.
- VPN required for login paths where documented (DUP §11.1).

Operational security

- Monitoring of utilisation, security events, and network traffic for operations and abuse detection (AUP §11, DUP §10.4).
- Graduated enforcement for policy violations including storage quarantine where justified (AUP §11.3, DUP §7.6).
- Vulnerability reports handled under AUP §7.4.

Availability and resilience

- Backups and retention as defined in DUP §8; not a substitute for Customer export before project end.

- Maintenance and disaster-recovery procedures in DUP §15.

Personnel and confidentiality

- PetaSC staff and contractors bound by confidentiality for data accessed during support or incident response.
- Access to Customer Personal Data limited to personnel with operational need.

Deletion

- Project and home data deleted per DUP §8.4–§8.7 after retention windows.
- Account LDAP records may be retained after access ends without reuse of UID/GID (DUP §3.6).

Customer-side measures

- The Customer shall implement organisation-appropriate measures for dataset encryption, pseudonymisation, and access control within project directories.

Appendix C — Document history

Version	Date	Author	Summary of changes
1.0	8 June 2026	Veselin Kolev <v.kolev@discoverer.bg> on behalf of PetaSC support team	Published: Article 28 DPA for Customer Personal Data on Discoverer; aligned with AUP §8 and DUP storage, identity, and retention rules