DELIVERABLE 11.1

POPD – REQUIREMENT NO. 1

WORK PACKAGE NUMBER: 11

WORK PACKAGE TITLE: ETHICS REQUIREMENTS

ETHICS

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Document Information

iReceptor Plus Project Information	
Project full title	Architecture and Tools for the Query of Antibody and T-cell Receptor Sequencing Data Repositories for Enabling Improved Personalized Medicine and Immunotherapy
Project acronym	iReceptor Plus
Grant agreement number	825821
Project coordinator	Prof. Gur Yaari
Project start date and duration	1st January, 2019, 48 months
Project website	http://www.ireceptor-plus.com

Deliverable Information	
Work package number	WP11
Work package title	Ethics requirements
Deliverable number	D11.1
Deliverable title	POPD – Requirement No. 1
Description	The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable.
Lead beneficiary	BIU
Lead Author(s)	Jos Dumortier, Liesa Boghaert

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Contributor(s)	
Revision number	
Revision Date	
Status (Final (F), Draft (D), Revised Draft (RV))	F
Dissemination level (Public (PU), Restricted to other program participants (PP), Restricted to a group specified by the consortium (RE), Confidential for consortium members only (CO))	CO

Approvals				
	Name	**Organisation**	**Date**	**Signature (initials)**
Coordinator	Prof. Gur Yaari	Bar Ilan University	30.06.2020	GY
WP Leaders	Prof. Gur Yaari	Bar Ilan University	30.06.2020	GY

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

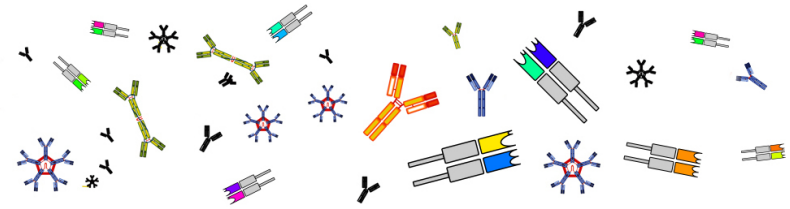
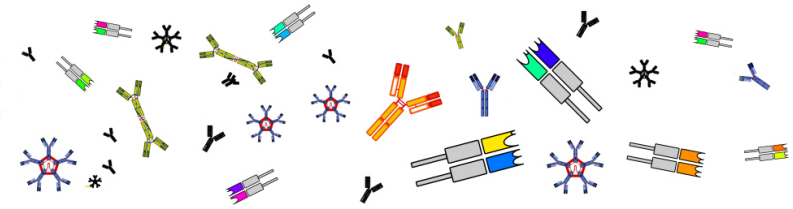


Table of Contents

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Executive Summary

D11.1 clarifies the role and tasks of a data protection officer and interprets POPD Requirement No. 1 in the context of the iReceptor Plus project. It confirms that each 'host institution', i.e. each entity contributing a repository to the iR+ network of repositories that is subject to the GDPR and is required to appoint a DPO pursuant to article 37 of the GDPR, has appointed a DPO. In addition, it designates a project-specific DPO that will oversee all data processing activities performed in iReceptor Plus research activities. The deliverable includes the contact details for each of these DPOS. The deliverable furthermore specifies the data protection policy applicable to the entities running a repository in iReceptor Plus that are not required to appoint a DPO pursuant to the GDPR.

The deliverable nevertheless argues that at the moment no special categories of personal data are processed in the course of the project, and any processing of such data, if it will happen, will only occur in later phases of the project. Such data processing activities are not yet certain, as the project will rely as much as possible on anonymous data. Although there is thus, at the moment, no need for a DPO to be assigned, the consortium aims to uphold the highest standards of security and data protection in the iReceptor Plus platform and has therefore provided the contact details of both a project-specific DPO and the DPOs of the 'host institutions' that can act expeditiously if necessary.

Lastly, the deliverable sheds a light on the application of POPD Requirement No. 1 in the future, when the iReceptor Plus platform will be exploited and available to the public.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Introduction

As a part of Work Package 11, POPD Requirement No. 1 requires confirmation that the host institution has appointed a Data Protection Officer (DPO) and that the contact details of this DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR, a detailed data protection policy for the project must be submitted as a deliverable.

The interpretation of POPD Requirement No. 1 and the term 'host institution' in particular is largely dependent on the objectives, organisational structure and the data processing activities of the iReceptor Plus project.

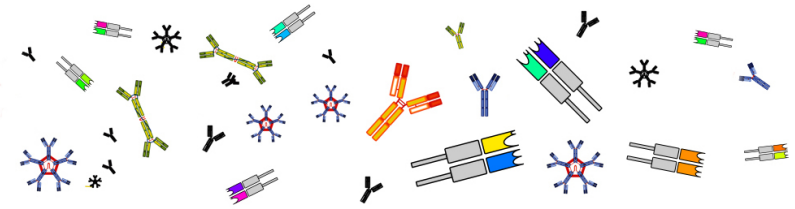
Therefore, this deliverable will start by setting out the objectives and structure of the iReceptor Plus project and clarifying the data processing activities performed in iReceptor Plus. In a following section, the deliverable will shed light on the concept of a Data Protection Officer and the tasks and responsibilities that come with this position. Then the deliverable will explain how POPD Requirement No. 1 should be interpreted in the context of iReceptor Plus and will communicate the contact details of the DPOs associated with iReceptor Plus. Moreover, it will specify the data protection policy applicable to the entities running a repository in iReceptor Plus that are not required to appoint a DPO pursuant to the GDPR. Lastly, the deliverable will comment on the application of POPD Requirement No. 1 in the future.

iReceptor Plus: objectives and structure

The iReceptor Plus project essentially intends to lower the barrier to share, access and analyse large sets of Adaptive Immune Receptor Repertoire sequencing data (AIRR-seq data) from around the world and to ease the availability of these AIRR-seq data to academia, industry and clinical partners. This increased availability of AIRR-seq data will advance the understanding of immune responses and may lead to the discovery of biomedical interventions (such as vaccines and other immunotherapies) that manipulate the adaptive immune system. Such advancements will enable improved personalized medicine and immunotherapy in cancer, inflammatory an autoimmune diseases, allergies and infectious diseases.

To this aim, iReceptor Plus will create a distributed network of repositories containing both AIRR-seq data and non-AIRR-seq data (such as clinical data, biological data, sample metadata, receptor reactivity data…). Via the 'iReceptor Plus Scientific Gateway', the end-user will be able to access, aggregate and analyse the data in the distributed repositories in order to study the global interactions within the immune system and its environment.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



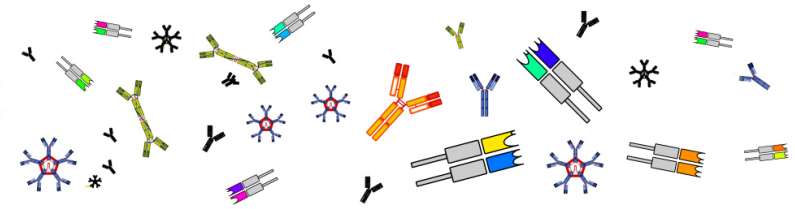
This data exploration, aggregation and analysis tool provided to researchers via the iR+ Scientific Gateway will allow researchers to pose complex queries about AIRR-seq data, their metadata and annotated sequence data. The Gateway then, on behalf of the end-user, will send the query to each of the repositories, will federate the results from each repository and present these federated results to the end-user. But the Gateway will go even further, as it will be able to stage federated data resulting from a query to an advanced analysis tool that uses computational methods on the aggregated data, such as relational datamining algorithms and deep learning techniques (AI), to facilitate complex analysis of the federated data and integrate it with other types of human health and genomic data.

The distributed nature of the iReceptor Plus network of repositories implies that **each research institution, hospital or other entity running a repository in iReceptor Plus maintains control over its own data and will be responsible for remaining compliant with its own local legislation**. The iReceptor Plus platform will merely serve as a tool which allows researchers to access, share, aggregate and analyse data from the repositories that are member to iReceptor Plus. It should thus be emphasized that all research institutions, hospitals or other entities that are part of iReceptor Plus remain fully in charge of the data in their repositories and that **iReceptor Plus will not create 'one large repository of AIRR-seq data and metadata' that includes the data from all of these repositories.**

Consequently, from an organisational perspective, **there will not be an overarching entity in iReceptor Plus that controls all data that will be accessible for analysis through the iReceptor Plus platform, and as such, there will not be one sole 'host institution'**, as mentioned in POPD-Requirement No. 1. **Rather, each research institution, hospital or other entity that 'connects' its repository to the iReceptor Plus Gateway should be considered as a host institution in the sense of POPD Requirement No. 1** , given that each of these entities will host the data in their repository in the cloud or local server of their own choice.

As matters stand, iReceptor Plus will connect repositories based in the EEA (France, Germany), Israel, Canada (British Columbia) and the United States of America (California and Texas). It is however envisaged that other repositories, from non-beneficiaries in this project may also be participating in the future, when the project is fully operational and accessible to the public.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



iReceptor Plus: Data processing activities

When looking at the data processing activities in iReceptor Plus, it is important to remember that the goal of iReceptor Plus is to create a software platform that enables (1) the querying of multiple repositories at once by metadata searches, (2) the analysis of federated data aggregated from multiple repositories and (3) the integration of these data with other types of large scale human health and genomic data. As mentioned above, these functionalities will be provided to the end-user via the iReceptor Plus Scientific Gateway.

The iReceptor Plus Scientific Gateway envisages to operate on three levels. First of all (1), it will give access to publicly available AIRR-seq data in the AIRR Data Commons ('public AIRR-seq data'). On a second level (2), the Gateway will provide an intermediate level of sharing of non-publicly available AIRR-seq data that can only be accessed if common consent structures or reciprocal data transfer agreements (DTA) are put in place ('controlled AIRR-seq data'). Finally (3), it will provide the ability to integrate public AIRR-seq data with non-public non-AIRR seq data (such as information extracted from individual electronic health records), without exposing the non-public non-AIRR seq data.

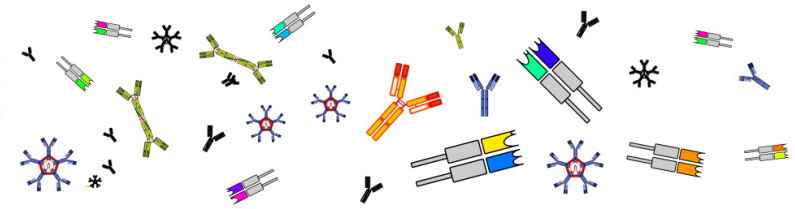
- The **public AIRR-seq data** (including metadata) are data that were originally used to perform scientific research, and which were afterwards deposited in a repository as a pre-requisite to the publication of the research paper the data support.

  In the context of iReceptor Plus, the individual repositories include public AIRR-seq data that come both directly from research studies performed by the scientific entity curating the repository as well as AIRR-seq data that were taken from other large repositories such as SRA[1] or ENA[2].

  Every deposit of AIRR-seq data into a repository is always performed under the supervision of and with the authorisation of the ethics committee responsible for the research data concerned. Each ethics committee is responsible for following ethical guidelines and complying with the GDPR and national data protection laws. Given that most national laws foresee an obligation of anonymisation before research data can be published and these large repositories like SRA and ENA often request a confirmation of anonymity from the contributor, the AIRR-seq data deposited in the public repositories should be considered **anonymous** and thus not subject to the provisions of the GDPR.

[1] The Sequence Read Archive (SRA) is a bioinformatics database that provides a public repository for DNA sequencing data, especially the 'short reads' generated by high-throughput sequencing, which are typically less than 1000 base pairs in length.
[2] The European Nucleotide Archive (ENA) is a repository providing free and unrestricted access to annotated DNA and RNA sequences.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



- The **controlled AIRR-seq data** (including metadata) are data that do not originate from publicly available repositories but come from research entities that have themselves performed the research concerned. Since those research entities were in contact with the people from whom the samples underlying the data were taken, they might be able to retrace the people to whom the data relate, unless anonymisation techniques were already applied to the data for publication purposes. This leads to the conclusion that some of the controlled AIRR-seq data **may be non-anonymous, personal** data and thus be subject to the provisions of the GDPR.

- The **non-public non-AIRR seq data** (including metadata) that can be integrated with public AIRR-seq data via the iReceptor Plus platform might be anonymous or non-anonymous data depending on the question if the entity curating these data has applied anonymisation techniques to the data. However, when integrating these non-public non-AIRR seq data with public AIRR-seq data, the non-public non-AIRR seq data will always remain with entity requesting the integration with the public AIRR-seq data and will never be shared with other parties. As such, the integration of non-public non-AIRR seq data with public AIRR-seq data via the iR+ platform will not amount to a processing op personal data, and will thus not trigger the applicability of the GDPR.

Needless to say, not all three levels of data access can realistically be developed at once and different data processing activities will occur in the different stages of development and exploitation. In fact, it is not entirely clear at the moment if the iReceptor Plus capabilities of sharing non-publicly available AIRR-seq data and integrating public AIRR-seq data with non-public non-AIRR-seq data will be developed and if so, this will only occur once the capability of sharing and analysing of public AIRR-seq data is functioning adequately. This means that only in the later stages of iReceptor Plus (M24-M48) personal AIRR-seq data might be processed. It is moreover not excluded that the iReceptor Plus consortium will make use of publicly available, anonymous AIRR-seq datasets for the second development phase of the iReceptor Plus tool.

Consequently, it is clear that the amount of actual personal data that will be processed in the first stages of the iReceptor Plus project (M1-M24) will be limited. It is only when non-anonymised, 'controlled AIRR-seq data' will be processed that the stringent data protection requirements of the GDPR may apply, and that the DPOs tasks and responsibilities will become more intense.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Section 4 of the GDPR: the Data Protection Officer (DPO)

Before addressing POPD Requirement No.1 to appoint a data protection officer in respect of iReceptor Plus, it is worthwhile to recall the provisions of the GDPR dedicated to the role of the data protection officer.

The GDPR devotes an entire section (Section 4, articles 37-39) to the role of the data protection officer. Whereas article 37 describes the circumstances in which a data protection officer should be designated, article 38 and 39 respectively elaborate on the position and tasks of the data protection officer.

In what follows, each of these provisions will be examined in more detail taking into account the Article 29 Working Party's 'Guidelines on Data Protection Officers ('DPOs')" of 2016 which have in the mean time been endorsed by the European Data Protection Board.

Article 37: Designation of the data protection officer

Article 37(1) of the GDPR requires controllers and processors to designate a DPO in three specific cases:

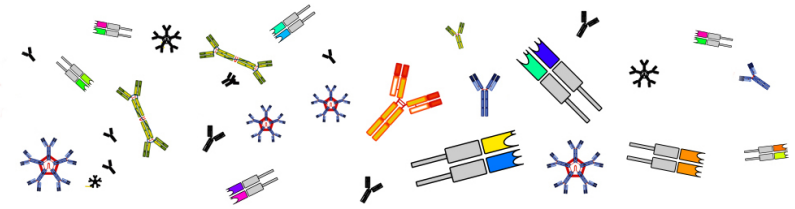
a) Where the processing is carried out by a public authority or body;
b) Where the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or
c) Where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

As regards this article, in light of the GDPR's accountability principle[3], the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. For iReceptor Plus, this deliverable can serve to that purpose.

In the context of iReceptor Plus, case c) of article 37(1) is most relevant: "a DPO should be designated where the core activities of the controller or the processor consist of processing on a large scale special categories of data or personal data relating to criminal convictions and offences."

[3] The accountability principle

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



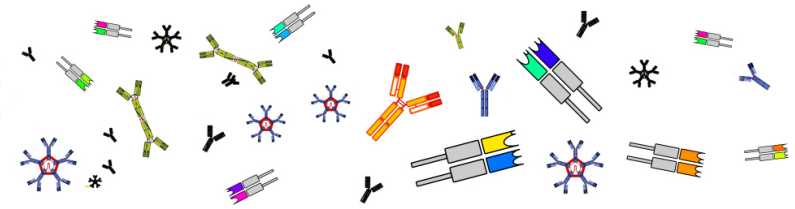
This is because if non-anonymous (and thus personal) AIRR-seq data would be processed in later stages of iReceptor Plus, either for the development of the tool's capability to access non-publicly available 'controlled AIRR-seq data' or after finalisation of the research project in the operational stage, that processing would be most likely be considered as 'a large scale processing of special categories of data' which constitutes one of the core activities of the research project or the entity that will later on supply the analysis tool developed by the iReceptor Plus consortium. This follows from the meaning of the terms 'core activities', 'large scale processing' and 'special categories of data' used in article 37.1.c:

> According to recital 97 of the GDPR, the 'core activities' of an organisation relate to the 'primary activities and do not relate to the processing of personal data as ancillary activities'. As such, core activities can be considered as the key operations necessary to achieve the controller's or processor's goals.
>
> 'Large scale processing' is however not defined in the GDPR. This is because it would be impossible to give a precise number either with regard to the amount of data processed or the number of individuals concerned for processing to be considered 'large scale' in all situations. The WP29 has nevertheless recommended some factors which should be considered in particular when determining whether the processing is carried out on a large scale. These are:
> - The number of data subjects concerned - either as a specific number or as a proportion of the relevant population;
> - The volume of data and/or the range of different data items being processed;
> - The duration, or permanence, of the data processing activity;
> - The geographical extent of the processing activity.
>
> 'Special categories of data' are data of which the processing is in principle prohibited pursuant to article 9.1 GDPR. These data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.

From these definitions, it is clear that any processing of non-anonymous (and thus personal) AIRR-seq data in later stages of iReceptor Plus would trigger the obligation to appoint a DPO under article 37.1.c) given the nature of the data (non-anonymous AIRR-seq data should be considered as genetic data, and thus special categories of data), the amount of data that would be processed (possibly thousand of sequences), the geographical extent of the processing activity (i.e. worldwide), the duration of the processing activity (i.e. for the duration of the project and possibly afterwards in case of exploitation of the research results).

As explained above, any processing of personal data, if it will take place, will occur in later stages of the project. In this respect, it should however already be mentioned that even if the

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



appointment of a DPO is not strictly necessary in accordance with article 37, nothing prevents an organisation from designating a DPO on a voluntary basis. In that case, the requirements under Articles 37 to 39 will still apply as if the designation had been mandatory.

Furthermore, it is noteworthy that Article 37(2) GDPR allows a group of undertakings to designate a single DPO, provided that he or she is "easily accessible from each establishment'. This accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority, but also within the organisation.

In any case, when the iReceptor Plus project is finalised and the data sharing and analysis tool is available to the public, a DPO will have to be appointed by the entity exploiting the tool, as this processor will process on a large scale special categories of personal data as a core activity, namely when it provides access to repositories containing non-publicly available, 'controlled' AIRR-seq data and metadata.

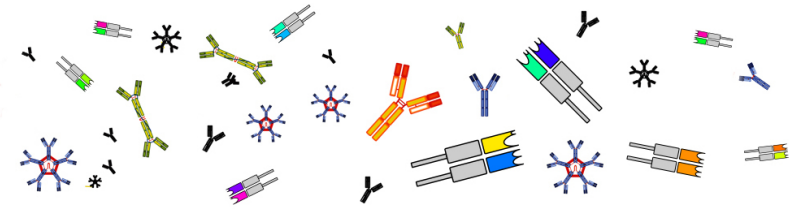
Article 37(5) emphasizes that a DPO 'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'. This necessary level of expert knowledge should pursuant to recital 97 GDPR be determined in accordance with the data processing operations carried out and the protection required for the personal data being processed.
According to the Article 29 Working Party:

- The required *level of expertise* must commensurate with the sensitivity, complexity and amount of data an organisation processes. Moreover, it may depend on whether the organisation systematically transfers personal data outside the EU or whether such transfer are occasional.
- In respect of *professional qualities*, DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GPDR. Knowledge of the business sector and of the organisation of the controller or processor is useful. Furthermore, the DPO should have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the organisation.
- The *ability to fulfil its tasks* refers to the personal qualities (such as integrity and high professional ethics) and knowledge of the DPOs, but also their position within the organisation.

Moreover, article 37(6) GDPR states that the data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

Lastly, article 37(7) GDPR requires the controller or the processor to publish the contact details of the DPO and to communicate the contact details of the DPO to the relevant supervisory authorities.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Article 38: Position of the data protection officer

Article 38 GDPR focuses on the position of the data protection officer in the organisation.

According to the first paragraph of article 38, controllers and processors should ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. This means that the DPO should be involved from the earliest stage possible in all issues relating to data protection.

Besides that, article 38(2) GDPR requires the organisation to support its DPO by 'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'. These resources could for example be active support by senior management, sufficient time to fulfil its duties, financial resources, infrastructure, staff…

Importantly, article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, DPOs should not receive any instructions regarding the exercise of their tasks and should not be penalised for performing their tasks. Whether or not they are an employee, the DPOs should be in a position to perform their duties and tasks in an independent manner. Nevertheless, it is the controller or processor, and not the DPO that remains responsible for compliance with data protection law and that must be able to demonstrate compliance.

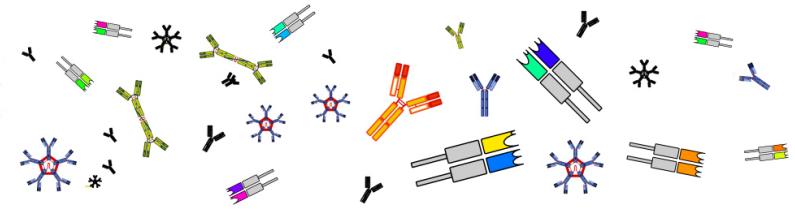
Interestingly, pursuant to article 38(6) GDPR, DPOs are allowed to fulfil other tasks and duties, provided that these tasks and duties do not result in a conflict of interests.

Article 39: Tasks of the data protection officer

In article 39 of the GDPR, the tasks of a DPO are listed. A DPO should:

- Inform and advise the controller or processor and employees who carry out processing of their obligations resulting from the GDPR or Member State data protection laws;
- Monitor compliance with the GDPR, other EU or Member State data protection provisions and the data protection policies of the controller or processor (including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and audits)
- Provide advice as regards the data protection impact assessment (when requested) and monitor the performance thereof;
- Cooperate with the supervisory authority;

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



- Act as the contact point for the supervisory authority on issues relating to processing (including prior consultation pursuant to Article 36) and to consult, where appropriate, with regard to any other matter.

When performing these tasks, DPOs should have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

iReceptor Plus and the requirement of designation of a DPO

Interpretation of POPD Requirement No. 1

Before elaborating on the interpretation of POPD Requirement No. 1 in the iReceptor Plus project, it is useful to recall the exact formulation of the requirement. POPD Requirement No. 1 states:

> *"The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable."*

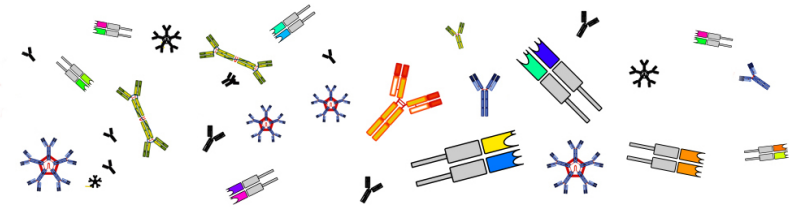
It follows from these wordings, that it is expected that 'the host institution' which hosts the personal data of data subjects, should appoint a DPO and should communicate the contact details of this DPO to the data subjects. Furthermore, if a host institution is not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable.

As was explained above, in iReceptor Plus, there is no overarching entity that hosts all data that can be found in the repositories taking part in iReceptor Plus. The project will not create one large repository of AIRR-seq data and metadata.

Rather, each research institution, hospital or other entity that 'connects' its repository to the iReceptor Plus Gateway should be considered as a 'host institution' in the sense of POPD Requirement No. 1 , given that each of these entities will host the data in their repository in the cloud or local server of their own choice. This follows from the distributed nature of the iReceptor Plus project, which implies that each research institution, hospital or other entity running a repository in iReceptor Plus maintains control over its own data and will be responsible for remaining compliant with its own local legislation. The iReceptor Plus project will only develop a platform or tool for accessing, aggregating, analysing and sharing the data in the distributed repositories.

This means that whenever a research institution, hospital or other entity that is based in the European Economic Area provides access to 'controlled' personal AIRR-seq data and metadata via the iReceptor Scientific Gateway, be it in the course of the research project for the development of the iR+ analysis tool, or afterwards when the tool is available to the public, that entity will have a 'large scale processing of special categories of data' as one of its core activities

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



and will pursuant to article 37.1.c of the GDPR be required to appoint a DPO. Therefore, all entities that are running a repository in iReceptor Plus and that are subject to the provisions of the GDPR have appointed a DPO. Other entities that are running a repository in iReceptor Plus but that are not subject to the GDPR's requirement of appointing a DPO, will comply with the data protection policy found in the last section of this deliverable.

Moreover, it might be that other consortium partners that don't run a repository in iReceptor Plus also process 'controlled', personal AIRR-seq data that they were given access to by the 'hosting entities' for the purposes of the project, namely the development of the iReceptor Plus platform. This constitutes a processing of special categories of personal data. However, it is quite unlikely that this would constitute a 'large scale' processing activity and will definitely not be the 'core activity' of that entity. As such, these entities are not required to appoint a DPO pursuant to the GDPR.

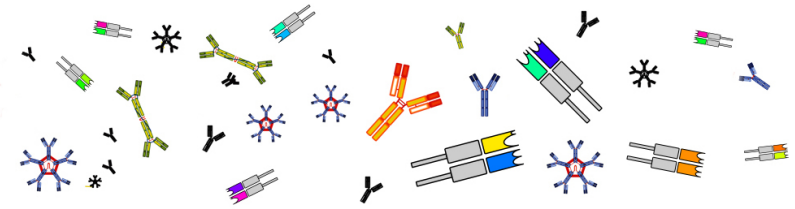
Nevertheless, if 'controlled', personal AIRR-seq data are processed in iReceptor Plus as a research project, the entirety of these processing activities will constitute a 'large scale' processing of 'special categories of personal data' which constitutes 'the core activities of the project'. Therefore, the iReceptor Plus consortium has decided to appoint a project-specific DPO, that will oversee all data processing activities in iReceptor Plus, even though strictly speaking, there is no overarching iReceptor Plus entity, but rather a consortium of research partners. Later on, in the exploitation phase of the project, when the iReceptor Plus tool is made available to the public, it will be up to the entity that supplies the iReceptor Plus tool to appoint a DPO.

Put concretely, the processing of personal data in the context of iReceptor Plus will be overseen by multiple DPO's.

> (1) First of all, all research institutions, hospitals or other entities that are subject to the provisions of the GDPR and that run a repository in iReceptor Plus have appointed a DPO that will oversee the personal data processing activities they perform. These entities are also responsible for communicating the contact details of the DPO to the data subjects concerned.
>
> (2) Secondly, the iReceptor Plus consortium will appoint a separate DPO that will oversee any personal data processing activities performed by non-repository-hosting partners in the iReceptor Plus consortium.

It should however be emphasized once more that the iReceptor Plus project will mainly concern the processing of anonymous 'publicly available' AIRR-seq data and metadata that were originally used to perform scientific research, and which were afterwards deposited in a repository in an anonymous way as a pre-requisite to the publication of the research paper the data support.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



The personal data processing activities of iReceptor Plus consortium partners will thus be very limited and can only concern the 'controlled AIRR-seq data and metadata' that do not originate from publicly available repositories but come from research entities that have themselves performed the research concerned. At present, these personal data are not processed by the consortium partners. The Scientific Gateway's capabilities of providing access to non-publicly available AIRR-seq data and integrating public AIRR-seq data with non-public non-AIRR-seq data will not be developed in the first stages of the project (M1-M24). This means that only in the later stages of iReceptor Plus personal AIRR-seq data might be processed. And even then, it is not certain that these personal data will be processed. If it is technologically meaningful, it might be that the scientific gateway's capability of providing access to non-publicly available AIRR-seq data and metadata will be developed and tested using publicly available, anonymous AIRR-seq data.

Nevertheless, due to the risk of re-identification of the data processed in iReceptor Plus, the consortium aims to uphold the highest standards of security and data protection on its platform. Therefore, it will voluntarily appoint a project-specific DPO, that will oversee the data processing activities performed throughout the project and that can act expeditiously should the processing of special categories of personal data be required in the development phase. This project-specific DPO will complement the work of the DPOs of each of the entities that are subject to the GPDR and that run a repository that is part of the iReceptor Plus platform.

In the following sections, the project-specific DPO and the DPOs of the entities required to appoint a DPO will be introduced, together with their contact details.

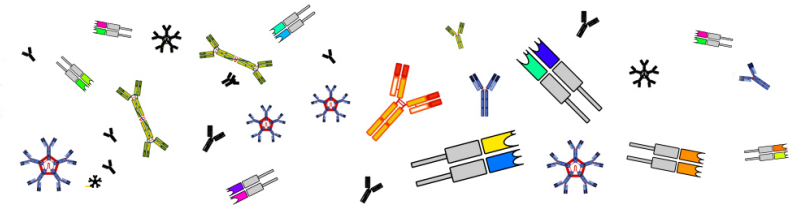
Project-specific DPO

The iReceptor Plus consortium appoints as the project-specific DPO Ms. Liesa Boghaert.
Ms. Liesa Boghaert can be contacted either via e-mail at liesa.boghaert@timelex.eu or via phone at +32 2 893 20 95 or +32 479 10 36 38.

Liesa Boghaert is an attorney-at-law in the Brussels-based law firm Timelex, one of the partners of the iReceptor Plus consortium. Since obtaining a Master's degree in Law (2017) and completing an additional Master's degree in Intellectual Property and ICT Law (2018), Liesa specialises in data protection, information technology, intellectual property and media law and advises clients in all of these fields. Liesa is furthermore affiliated with Ghent University as a teaching assistant for the courses data ethics, protection of health and genomic data and health innovation and law.

Timelex as a lawfirm is specialised in information and technology law in the broadest sense, including privacy protection, data and information management, e-business, intellectual property and telecommunications. Its activities cover all legal issues encountered in the creation, management and exploitation of information and technology, in all of its diverse forms.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



The Timelex team is internationally recognised, being both a Legal 500 Top Tier firm in Information Technology, and a Chambers Europe Recommended Firm for TMT - Information Technology, Intellectual Property, Data Protection and Entertainment. Time.lex has a proven track record in every aspect of information and technology law, from an academic, business and policy perspective.

Timelex is specifically known for its European policy studies in a variety of subjects, including data protection, electronic signatures, electronic identity management, e-business and e-government, in which they can rely on an extensive network of IT law experts covering all European countries. From a business perspective, Timelex frequently assists companies in establishing suitable policies and legal frameworks in their data management activities, including with regard to the cross-border transfer and processing of personal data, data security and liability management issues. Its clients include private companies and public sector bodies in the IT sector, financial services, e-health, marketing and e-commerce.

In iReceptor Plus, Timelex takes care of the legal and regulatory aspects, in particular with regard to privacy and personal data protection (WP3). The Timelex lawyers provide guidance to the "data protection by design" approach of the RIA, ensure GDPR compliance of the proposed solutions and deal with all other legal issues in the framework of the Action.

DPOs of partners contributing a repository

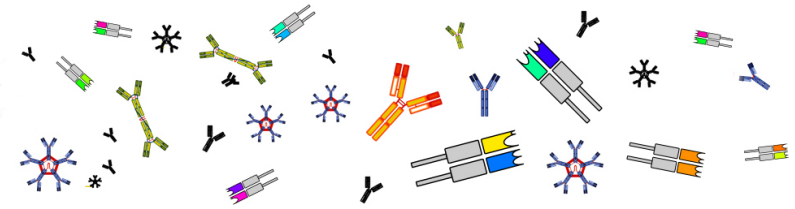
As was mentioned above, consortium partners that are bringing a repository to iReceptor Plus and that are subject to the GDPR, will be obliged to appoint a DPO if they process special categories of personal data on a large scale as their core activities.

This raises the question which consortium partners that contribute a repository to iReceptor Plus are subject to the GDPR.

Territorially, the GDPR applies to:

1. the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union,
    b. the monitoring of their behaviour as far as their behaviour takes place within the Union.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Given that iReceptor Plus as a research project does not perform any processing activities related to the offering of goods or services to data subjects in the Union, or to the monitoring of their behavior within the Union, the consortium partners that are established outside the European Union are not subject to the GDPR.

To the extent that the consortium partners that are established in the European Union process personal data in the context of the activities their establishment, they are subject to the GDPR, regardless of whether the processing takes place in the Union or not.

Consequently, all EU or rather EEA[4] consortium partners that contribute a repository to iReceptor Plus will be subject to the GDPR and will be required to appoint a DPO to the extent that processing special categories of personal data on a large scale is one of their core activities. These partners are:

- Assistance Publique hôpitaux de Paris (APHP) France
- German Cancer Research Center (DKFZ) Germany

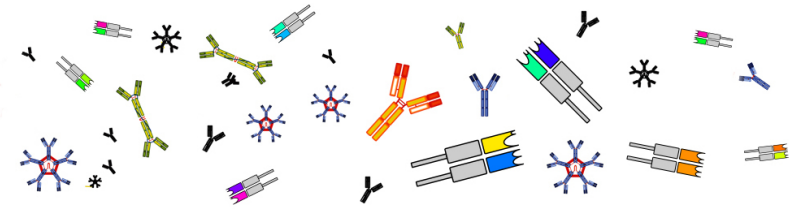
Assistance Publique hôpitaux de Paris (APHP)

The data protection officer of the Assistance Publique hôpitaux de Paris is Mr. Didier Perret. Mr Perret can be contacted either via e-mail at didier.perret@aphp.fr or at protection.donnees.dsi@aphp.fr.

The Clinical Investigation Centre in Biotherapy and Immunology (CIC-BTi) is a translational unit that conceives and performs clinical trials in biotherapy, i.e. investigating biologic-, cell- or gene-based therapies. This structure is part of the APHP, the public hospital system of the city of Paris and its suburbs. The CIC-BTi is specialized in developing immunotherapies, with a focus on Treg and low dose IL2 (ld-IL2) therapy. Since 2012, the CIC-BTi is fully implemented within two main national programmes: the laboratory of excellence Transimmunom (https://www.transimmunom.fr/en/) and the Hospital University department i2B (www.dhu-i2b.fr) which gathers 30 medical departments and 11 research teams from 4 University hospitals: Pitié-Salpêtrière, Tenon, Trousseau and Saint-Antoine. In this context, the CIC-BTi assembles a unique and significant workforce with multidisciplinary skills covering a continuum of inflammatory and autoimmune diseases (IADC). The purpose of CIC-BTi is to contribute to the development of clinical investigations aimed at better understanding the IADC, discovering novel targets for immune-intervention and exploiting new therapies starting with ld-IL2. For this, two major complementary approaches have been developed: i) the cross evaluation of clinical,

[4] The General Data Protection Regulation (GDPR) (EU) 2016/679 entered into force in Iceland, Liechtenstein and Norway on 20 July 2018. The Joint Committee Decision (JCD) incorporating the GDPR was adopted by the EEA Joint Committee on 6 July 2018 and entered into force on 20 July 2018.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



biological and multi-OMICs data in patients of the IADC using systems biology methodologies and ii) the cross-study of ld-IL2 in several conditions of the IADC, including deep phenotyping of patients.

CIC-BTi, as the legal "owner" of patient information, will provide access to the Transimmunom AIRR-Seq project. This data will become available to the public, and in turn made available through the iReceptor Gateway (WP1), once the results of this work has been published. In addition, AP-HP will be responsible for the integration of clinical data together with the AIRR-Seq, as described in WP6.

German Cancer Research Center (DKFZ)

The data protection officer of the German Cancer Research Center is Mr Michael Westermann. Mr Westermann can be contacted either via e-mail at m.westermann@dkfz-heidelberg.de or via phone at +49 6221/421673.

The German Cancer Research Center (Deutsches Krebsforschungszentrum, DKFZ) is an independent non-university academic institution within the Helmholtz Association. It is the largest biomedical research institution in Germany and one of Europe's largest cancer research centers. Its mission is to unravel the causes and mechanisms of cancer development and progression and to develop novel strategies for prevention, early detection, diagnosis and treatment through innovative translational cancer research.

Capitalizing on its long-standing expertise with single-cell data, in iReceptor Plus, DKFZ will be responsible for all activities related to single-cell AIRR-seq and associated data types. The majority of these activities, like the development and implementation of a common single-cell data standard and a generic import mechanism for single-cell AIRR-seq data, are bundled in WP7. This WP also deals with the tight integration of flow cytometric and receptor reactivity data in the database. Furthermore, within WP2, the integration of the single-cell database into the iReceptor network is also assigned to DKFZ.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Data protection policy for iReceptor Plus

In accordance with POPD Requirement No.1, the non-EEA partners that will connect their repository to iReceptor Plus will act in accordance with the data protection policy included below, to the extent that they are processing (special categories of) personal data. These partners are:

- Bar Ilan University (BIU)	Israel
- Simon Fraser University (SFU)	Canada
- University of Haifa (UH)	Israel
- Medgenome (MEDGENOME)	United States of America
- University of Texas Southwestern Medical Center (UTSW)	United States of America

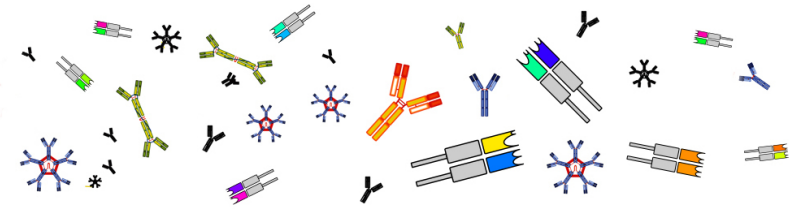
Data protection policy iReceptor Plus

In this section of the deliverable, the iReceptor Plus Partners wish to outline their data protection policy ("Policy") for complying with POPD Requirement No.1. Due to the many stakeholders active in different capacities and sectors, this Policy has been drafted on the basis of the GDPR. It outlines the minimal rules to be observed by the partners to ensure compliance. Partners will adhere to their own internal data protection policies for the processing activities taking place in the context of the iReceptor Plus project. These policies should not lessen, diminish or disapply the measures put forth herein.

1. Definitions

1) **Consortium Agreement**: the agreement of 1 January 2019 concluded between the beneficiaries of the Grant Agreement for the performance of the action as described in the DoA and any change, update or amendment thereof.
2) **DoA**: the description of the action as annexed to the Grant Agreement and any approved update or amendment thereof.
3) **Grant Agreement**: the agreement of 8 December 2018 with no. 825821 concluded between the European Union, represented by the European Commission, and the Partners.
4) **Partner**: a beneficiary identified in the Grant Agreement and a signatory to the Consortium Agreement.
5) **Project**: the iReceptor Plus action as described in the DoA.
6) The terms "personal data", "data subject", "controller", "processor", "processing" and "personal data breach" shall have the same meaning as in Article 4 GDPR. The terms

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



"special categories of personal data", "data protection impact assessment", "prior consultation" and "transfer of personal data" shall have the same meaning as in Articles 9, 35, 36 and 44 GDPR respectively.

2. General

Whether a Partner acts as controller or processor in the context of the Project, it shall at all times endeavor to observe the measures outlined in this Policy and assist, where reasonable and relevant taking into account that Partner's role and the information available to it, the other Partners to do the same.
Each Partner shall ensure that its staff members and contractors, as well as anyone who processes personal data on that Partner's behalf, is made aware of the measures stipulated in this Policy.

3. Observing the data protection principles

All Partners, when acting in their capacity of controller for the processing personal data in the context of performing their tasks as listed in the DoA, shall observe the following data protection principles:

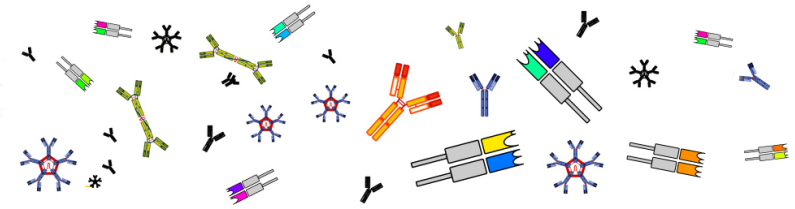
Lawfulness, fairness and transparency: each personal data processing activity undertaken in the context of the Project shall have a legal basis for processing, shall be communicated and explained to data subjects and shall not go beyond what the data subject may reasonable expect from the processing activity based on what has been communicated by the Partner.

In the event that multiple Partners are involved in a data processing activity and no contractual arrangement concerning providing information to data subjects has been put in place, the Partner appointed in the DoA as leader for the task in the context of which the data processing activity takes place shall be responsible for ensuring that adequate information notices are provided to the data subjects concerned.

Where the data processing activity involves the consortium as a whole, the Project's coordinator shall bear this responsibility. All Partners involved in such a data processing activity will provide the information and input requested as well as the active assistance required to draft and communicate such information notices.

Purpose limitation: taking into account its rights and obligations under the Grant Agreement and the Consortium Agreement, each Partner will process personal data collected in the context of the Project for the specific, explicit and legitimate purposes necessary to perform its tasks as defined in the DoA, in accordance with what has been communicated to the data subject and not

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



further in any way that is incompatible with those purposes.

Data minimization: each Partner will only process personal data in the context of the Project only insofar these personal data are adequate, relevant, not excessive and necessary to achieve the purposes for processing which allow the Partner to perform its tasks in the DoA. This means, among others, that personal data in public deliverables and open data sets will be anonymized or at least pseudonymized wherever possible.

Accuracy: each Partner will ensure that personal data processed in the context of the Project are accurate, complete and kept up to data and that its processing activities are set up in such a way that compliance with this principle can be assured for the whole duration of the project.

Storage limitation: taking into account the obligations as set out in the Grant Agreement, particularly related to open access and data management, each Partner will ensure that personal data are only stored as long as required for the purposes for which they were processed in the context of the Project and only further processed insofar the purposes for further processing are compatible with the original purposes.

Integrity and confidentiality: each Partner will ensure that the personal data it processes in the context of the Project is kept safe and confidential. To that end, each partner shall minimally take the measures outlined in section 5 of this Policy. Each Partner shall take the necessary measures to ensure that anyone who processes personal data on that Partner's behalf is bound by a statutory or contractual confidentiality obligation.

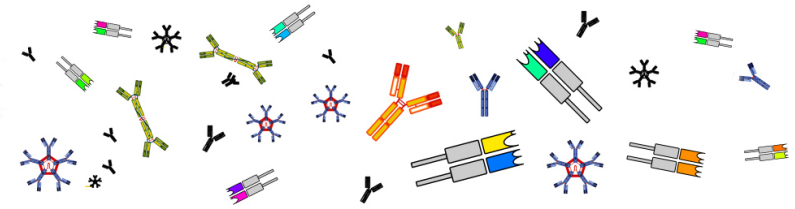
4. Legal basis for processing

Every personal data processing activity in the context of the Project shall be based on at least one legal basis for processing as outlined in Article 6 GDPR. It is up to the Partner acting as controller to determine the appropriate legal basis for processing personal data for a particular purpose:

Where personal data processing is based on **consent**, the Partner will use an information notice which minimally contains the following elements:

1) the controller's identity;
2) the purpose of each of the processing operations for which consent is sought;
3) what (type of) data will be collected and used;
4) the existence of the right to withdraw consent;
5) information about the use of the data for automated decision-making where relevant; and

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



6) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards.

When and where required to perform the tasks set out in the DoA, Partners will obtain consent on behalf of the other Partners which are involved in the such tasks.

Where personal data processing is based on the necessity of such processing to **conclude an agreement** with the data subject or to **perform an agreement** with the data subject, the Partner will ensure that the processing is objectively necessary for a purpose that is integral to the conclusion of the contract or for the performance of the obligations arising out of the contract.
Where personal data processing is based on the necessity of such processing to comply with a **legal obligation**, the Partner shall limit its processing to what is required to comply with such legal obligation.

Where personal data processing is based on the necessity of such processing for the purposes of the **legitimate interests** pursued by the Partner or a third party, the Partner shall undertake a balancing test to ascertain whether those legitimate interests are not overridden by interests or fundamental rights and freedoms of the data subject.

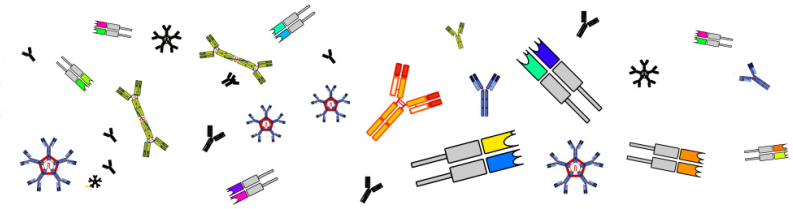
Where personal data are **further processed** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the Partner will take appropriate safeguards which shall at minimum include the measures listed in section 5 of this Policy.

5. Appropriate technical and organizational measures

Each Partner processing personal data in the context of the Project, either as controller or as processor, will minimally take the following measures:

1) deny unauthorised persons access to processing equipment used for processing ('equipment access control');
2) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
3) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');
4) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
5) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



6) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
7) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
8) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
9) ensure that installed systems may, in the case of interruption, be restored ('recovery');
10) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity')

6. Data protection by design and by default

Each Partner will ensure that the personal data processing activities it intends to undertake in the performance of its tasks as outlined in the DoA are designed and implemented in a manner that integrates the data protection principles outlined in section 3 and the measures outlined in section 5 of this Policy.

When required, Partners will use the different consultation and collaboration mechanisms created and agreed upon in the course of the Project to ensure that data protection by design and by default are observed in all collaborative tasks in the different work packages as described in the DoA.

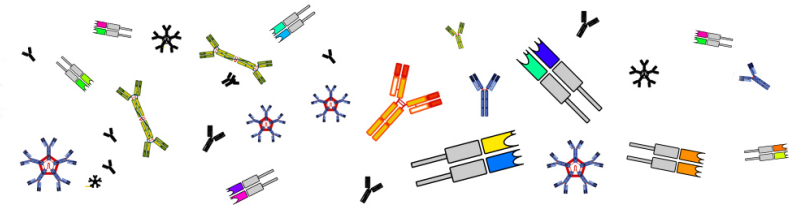
7. Third party relationships

7.1 Use of (sub-)processors

Whenever a Partner, acting as controller, relies on a processor for the processing of personal data in the context of the Project, such Partner shall assess whether the processor provides sufficient warranties and safeguards for the processing of personal data. If the Partner deems the warranties and safeguards offered sufficient, the Partner will conclude a contract with the processor which covers at minimum all of the topics listed in Article 28.3 GDPR.

Whenever a Partner, acting as a processor, relies on a sub-processor for the processing of personal data in the context of the Project, it shall assess whether the sub-processor offers

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



warranties and safeguards which are the same or equivalent to the warranties and safeguards the Partner itself offers. If the Partner deems the warranties and safeguards offered equivalent, the Partner will conclude a contract with the sub-processor which incorporates the same or equivalent obligations that the Partner has vis-à-vis the controller.

7.2 Exchanging personal data with recipients

Exchanging personal data with recipients which are not Partners or processors shall only happen in accordance with the obligations and constraints in the Grant Agreement and the Consortium Agreement. Each Partner is aware of the fact that such exchange constitutes a separate processing activity which requires a legal basis for processing and for which all data protection principles must be observed.

7.3 Joint controllership

When two or more Partners are all responsible as joint controllers for a data processing activity, they shall conclude a data sharing agreement which governs their mutual rights and obligations as joint controllers. Such Partners shall observe that:

1) the information notices towards data subjects contain the required information concerning the joint controllership; and
2) their records of processing activities reflect the joint controller relationship.

8. Record of data processing activities

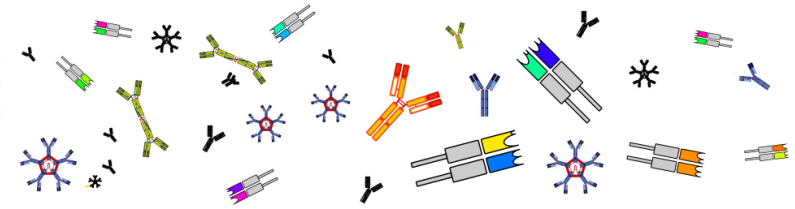
Each Partner, as controller or as processor, shall keep its own record of data processing activities undertaken in the context of the Project. Partners shall, where required, assist each other to keep their records accurate, complete and up to date.

9. DPIA and prior consultations

Each Partner, acting as controller, is responsible to assess whether a data processing activity carried out in relation to a task as described in the DoA requires a DPIA or a prior consultation. The Partner shall choose the most appropriate methodology to undertake a DPIA, including but not limited to the templates and methodologies developed by the national data protection authorities.

When such data processing activity involves multiple Partners and no contractual arrangement concerning DPIAs and prior consultations has been put in place, the Partner appointed in the DoA as leader for the task in the context of which the data processing activity takes place shall be

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



responsible for coordinating the DPIA or prior consultation.

When the data processing activity involves the consortium as a whole, the Project's coordinator shall coordinate the DPIA or prior consultation. All other Partners involved in such data processing activity shall actively contribute to, and shall provide all input required for, the timely undertaking of such DPIA or prior consultation.

10. Data subject rights

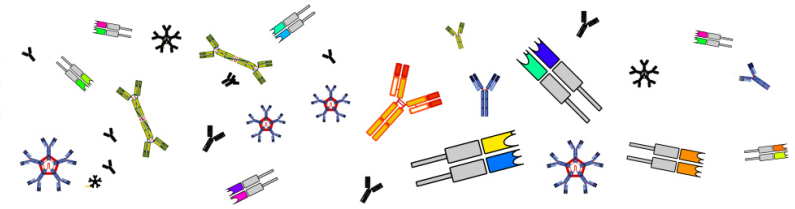
Each Partner acting as controller shall be responsible to observe the rights of the data subjects whose personal data such Partner processes.

In the event it is no longer possible to ascertain which Partner is responsible for the processing activity, the Project's coordinator shall serve as the main contact point for requests of data subjects. It will be up to the Project's coordinator to refer the request to the appropriate Partner(s).

Partners shall ensure that for all data processing activities undertaken in the context of the Project, the following data subject rights are observed at all times:

1) **Right of access**: the data subject may request access to the personal data concerning him/her and is entitle to information concerning the purposes of the processing, the recipients to whom the personal data are transferred and, where possible, the envisaged period for which the personal data will be stored.
2) **Right to rectification**: the data subject has the right to request without delay the rectification of inaccurate or incomplete personal data concerning him or her.
3) **Right to erasure** ("right to be forgotten"): the data subject has the right to have personal data of him erased without unreasonable delay when one of the following applies:
    a. the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
    b. the data subject withdraws the consent on which the processing is based, and there is no other legal basis for the processing;
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes;
    d. the personal data have been unlawfully processed;

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



e. personal data must be deleted in order to comply with a legal obligation incumbent on the controller;

f. the personal data were collected on the basis of the consent of a minor under thirteen (13) in connection with an offer of information society services (i.e. online services such as mobile or online apps).

4) **Right to restriction** of processing: in some situations, the data subject has the right to request the restriction of the processing of his or her personal data. This right can only be invoked where one of the following situations applies:

a. the accuracy of the personal data is contested by the data subject for a period enabling us to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c. our company no longer needs the personal data for the purposes of the processing, but the data subject still needs the personal data in the context of legal proceedings or;

d. the data subject has objected to the processing, pending the answer to the question whether the legitimate grounds of our company outweigh those of the data subject.

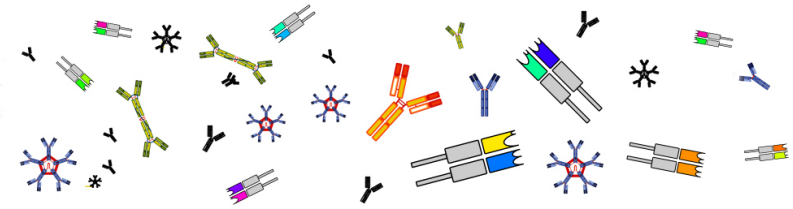
5) **Right to data portability**: if the processing of personal data is based on the consent of the data subject, on the performance of the contract between a Partner and the data subject and if the processing is carried out by automated processes, the data subject has the right to obtain the personal data that he or she has provided to us in a structured and commonly readable form and to transfer those data to another controller.

6) **Right to object**: if the processing is necessary to pursue the legitimate interest of our company or a third party (or if the processing is necessary for the performance of a task carried out in the public interest), the data subject may object the processing, unless the Partner demonstrates compelling legitimate interests for the processing which override the interest, right or freedoms of the data subjects or for legal claims.

7) **Right not to be subject to automated individual decision-making**: the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her.

8) **Right to withdraw consent**: the data subject has the right to withdraw its previously granted consent. Withdrawing consent should be as simple as granting consent.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



11. Personal data breach management and notification

All Partners will implement a personal data breach management and notification procedure within their respective organizations.

When a personal data breach concerns a data processing activity to which multiple Partners participate and no contractual arrangement governing management and notification of personal data breaches has been put in place, the Partner appointed in the DoA as leader for the task in the context of which the data processing activity takes place shall be responsible for coordinating the data breach management and notification processes. The final decision to notify shall be made by the Partner acting as task leader, but the opinions of the Partners involved shall be taken into account.

When the data processing activity involves the consortium as a whole, the Project's coordinator shall coordinate the data breach management and notification processes. All other Partners involved in such data processing activity shall actively contribute to, and shall provide all input required for, the mitigation of the effects of the personal data breach and the notification of such breach to data protection authorities and, where appropriate, data subjects. The final decision to notify shall be made by the Project's coordinator, who will take the opinions of the Partners involved into account.

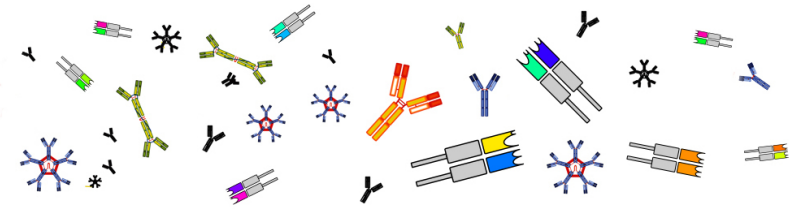
12. Cooperation with the data protection authorities

All Partners shall actively respond to requests from, and cooperate with, the competent data protection authorities in the exercise of their tasks and supervisory powers.

When a request or duty to cooperate relates to a data processing activity to which multiple Partners participate and no contractual arrangement governing contact with data protection authorities has been put in place, the Partner appointed in the DoA as leader for the task in the context of which the data processing activity takes place shall act as point of contact for the competent data protection authorities.

For data processing activities concerning the whole consortium, the Project's coordinator shall act as the primary point of contact for the competent data protection authorities.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Conclusion and future work

This deliverable explained the concept of a data protection officer and interpreted POPD Requirement No. 1 in the context of the iReceptor Plus Project. Confirmation is given that each 'host institution' that is subject to the GDPR and is required to appoint a DPO pursuant to article 37 of the GDPR, has appointed a DPO. In addition, a project-specific DPO has been appointed to oversee the data processing activities performed in iReceptor Plus research activities. The deliverable includes the contact details for each of these DPOs and specifies the data protection policy applicable to the entities running a repository in iReceptor Plus that are not required to appoint a DPO pursuant to the GDPR.

Nevertheless, the deliverable argues that at the moment no special categories of personal data are processed in the course of the project, and any processing of such data if it will happen, will only occur in later phases of the project. Such data processing activities are not certain yet, as the project will count as much as possible on anonymous, public data. Although there is thus at the moment, no need for a DPO to be assigned, the consortium partners aim to uphold the highest standards of security and data protection on the iReceptor Plus platform and have therefore provided the contact details of both a project-specific DPO and the DPOs of the 'host institutions'.

The deliverable does however acknowledge that whenever a new repository will be added to the iReceptor Plus distributed network of repositories in the future (when the iReceptor Plus tool is exploited), it will have to be assessed if the entity giving access to this repository is subject to the GDPR and if it is required to appoint a DPO pursuant to article 37 GDPR. Moreover, the same assessment will have to be made in regards the entity that supplies the iReceptor Plus platform itself to the public.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)