This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061

Advanced Tools for fighting Online illegal trafficking

D3.6 – LEAs Cooperation Policy - update

WP number and title	WP3 – Social, Ethical, Legal and Privacy issues of online sources analysis
Lead Beneficiary	IIP
Contributor(s)	IIP
Deliverable type	Report
Planned delivery date	30/04/2020
Last Update	21/05/2020
Dissemination level	PU

Disclaimer

The ANITA Consortium consists in the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Engineering Ingegneria Informatica	ENG	IND	IT
2	Centre for Research and Technology Hellas CERTH - ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	RTO	GR
3	Centro Ricerche e Studi su Sicurezza e Criminalità	RISSC	RTO	IT
4	Expert System S.p.A.	EXPSYS	SME	IT
5	AIT Austrian Institute of Technology GMBH	AIT	RTO	AT
6	Fundacio Institut de BioEnginyeria de Catalunya	IBEC	RTO	ES
7	Istituto Italiano per la Privacy	IIP	NPO	IT
8	SYSTRAN SA	SYSTRAN	SME	FR
9	Stichting Katholieke Universiteit Brabant	TIU-JADS	RTO	NL
10	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
11	VIAS Institute	VIAS	RTO	BE
Law Enforcement Agencies (LEAs)				
12	Provincial Police Headquarters in Gdansk	KWPG	USER	PL
13	Academy of Criminalistic and Police Studies – Kriminalisticko-Policijska Akademija	AoC	USER	RS
14	Home Office CAST	CAST	USER	UK
15	National Police of the Netherlands	NPN	USER	NL
16	General Directorate Combating Organized Crime, Ministry of Interior	GDCOC	USER	BG
17	Local Police Voorkempen	LPV	USER	BE

To the knowledge of the authors, no classified information is included in this deliverable

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	20/02/2020	Draft	IIP	First draft
V0.2	11/03/2020	Draft	IIP	Second draft
V0.3	06/04/2020	Draft	IIP	Third draft
V1.0	30/04/2020	Draft	IIP	Fourth Draft
V1.1	21/05/2020	Definitive	IIP, NPN	Version ready to be submitted

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
DPO	Data Protection Officer, the natural person appointed, by the Data Controller or the Data Processor in the cases set forth by Art. 37.1 GDPR, who has specific knowledge and competence regarding data protection regulations and practices to assist the Data Controller or the Data Processor in complying with the GDPR;
GDPR	General Data Protection Regulation 2016/679
LEA	Law Enforcement Agency
UC	Use Cases
WP	Work Package
Archive	any structured set of Personal Data which is accessible according to specific criteria, whether centralised, decentralised or distributed on a functional or geographical basis;
Automated Decision Making	decisions based only on automated Processing, including Profiling, that produce legal effects concerning the natural person or similarly significantly affect the natural person;
Biometric Data	Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data;
Common Data	any Personal Data which are not included in Special Categories of Personal Data or Judicial Data;
Consent of the Data Subject or Consent	any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she signifies, by means of a statement or by a clear affirmative action, agreement to the Processing of Personal Data relating to him or her;
Corporate Equipment	any Desktop Device and Mobile Device given to Persons Authorised by the undertakings in order to carry out their professional duties;
Computer LEAs Network	the digital perimeter of the undertakings possibly containing Personal Data and/or confidential information. It consists in hardware and software tools for the management of both internal services (e.g., switch, LAN, Wi-Fi) and external inbound or outbound connections (e.g. boundary router, SSH, VPN);

Cross-border Processing	a) Processing of Personal Data which takes place in the context of the activities of establishments in more than one Member State of a Data Controller or a Data Processor in the Union where the Data Controller or the Data Processor is established in more than one Member State; or (b) Processing of Personal Data which takes place in the context of the activities of a single establishment of a Data controller or a Data Processor in the Union but which substantially affects or is likely to substantially affect Data Subjects in more than one Member State;
Data Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Data Processor	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller; providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Regulation and ensure the protection of the rights of the Data Subject;
Desktop Device	any hardware that cannot be easily removed from the perimeter of the undertakings, such as personal computer, local servers, printers assigned to Persons Authorised for professional use;
Judicial Data	Personal Data relating to criminal convictions and offences or related to security measures;
Mobile Device	any IT hardware that is easily removable form the perimeter of the undertakings such as USB sticks, SD cards, external hard disks, tablets and smartphones used by the Persons Authorised for professional use;
Personal Data Breach	any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed;
Personal Data	any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Processing	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Recipient/s	a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as Recipients; the Processing of that data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the Processing;
Special Categories of Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of Genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data concerning Health or data concerning a natural person's sex life or sexual orientation;
Supervisory Authority	independent public authority of a Member State under Art. 51 GDPR;

Table of Contents

Executive Summary

This policy is drafted to tackle the issue of misuse, and to facilitate the LEAs in addressing known issues related to the proper collaboration necessary to carry out procedures for compliance with data protection legislation.

Purpose of the policy

In the current era of globalization, characterized by the globalization of information, there is a strong need to ensure international police cooperation in preventing and fighting increasingly transnational criminal offences perpetrated via the Internet, and in particular through dark web.

Considering the ease with which criminals or criminal groups collaborate within the territory of more than one State, it is inevitable to eliminate or in any case mitigate those legal and administrative obstacles that prevent a prompt response at international level.

The purpose of this policy is to assess the current state of international police cooperation through a critical analysis of the main legal instruments used to establish collaborative relations between law enforcement agencies of different States and to properly address how to collaborate using ANITA as a tool to prevent and fight criminal activities.

In particular, the policy has the aim of favoring the coordination of the national law enforcement agencies in carrying out activities of prevention and fight against certain criminal cases of trans-national importance individuated and detailed in the use cases scenarios.

The legal instruments *de quo* are not the only instruments to promote such cooperation.

ANITA, as such, could be considered as a practical tool to facilitate collaboration, regardless of the framework in which it operates.

The investigative potential of ANITA needs a set of pre-established rules which can effectively mitigate possible misuses of the tool for the creation of a direct and constant form of cooperation between the police of the various States, in order to facilitate the capture of criminals settled abroad during the commission of criminal offences. The pre-established rules have been drafted in order to allow LEAs' cooperation as described in section 4 of the present policy, following the principles of the EU legal framework; in particular this according to the rules set forth by Chapter III of the Budapest Convention on Cybercrime of 23rd November 2001.The exchange of information between police forces is not developed in the digital age for the first time, but it is considered fundamental since the dawn of the European community, more than a century ago. The oldest example in Europe of a formal agreement between States for the exchange of information in police investigation is the initiative of Austria, Belgium and the Netherlands in Hamburg in 1888 to establish a cooperation against crimes through a dense exchange of information. In this regard, in the course of the successive decades, the increase of juridical instruments which have allowed the police of the European States to collaborate effectively in the prevention of crime, has grown exponentially and thus ANITA can be considered one of the highest points of successful cooperation between States for crime prevention purposes.

Nevertheless, it is of paramount importance to regulate the cases that may occur to the LEAs in the use of ANITA even during the initial phase of development of the tool. In this regard, this collaboration policy has been drafted, including 5 different sections. The first addresses the issue of misuse, i.e. the possibility of using ANITA for inappropriate purposes and for purposes that are not in line with the ethics, European Union legal framework and EU member State national law. The second section concerns the incident handling and data breach, i.e. the formalization of a possible procedure to deal with the violation of personal data. The third concerns the cooperation with the data protection authority in case of inspection and the necessary coordination between the LEAs and the DPO of the project. The fourth section deals with the main cooperation rules to be considered when using the tool and the fifth section contains the annexes with the documents that should be drafted when a data breach occurs.

1 Cooperation in avoiding misuse

1.1 Use against the law

a) LEA's operators are professionals who have technical and substantive expertise and who work with ethical standards. During the performance of their activities, LEA's operators shall comply with ethical standards and with national and European laws. In particular, in the majority of the cases, LEA's operators shall comply with the law of the Country in which they are operating, and, in general, with all applicable European laws. This applies to a range of legal frameworks, including but not limited to privacy, human rights and criminal law. LEAs' operators shall not put themselves in a situation in which they may contravene such laws.

b) Notwithstanding the provision of the precedent paragraph, there are occasionally situations in which to explore a particular issue, LEA's operators may be involved in activities that could break the law[1]. In these cases, when utilizing the tool in a way that could pose the LEA's operators in an illegal situation, it is important to balance the need for the information with the possible personal danger and to evaluate if data collected are necessary. In some cases, this could be clear and can help the authorities to deal with them, for crime prevention and to carry out investigations. In others, it is less clear whether the information is needed or not.[2]

c) In this context, a distinction shall be made between whether LEAs operators are operating during the 1st phase: the "**Research Phase**" or during the 2nd phase: the "**Exploitation Phase**" when there will be the deployment of the tool. In the first phase, if ethical and legal doubts should arise for an operator of the LEAs, this operator, directly or through a superior, shall activate the DPO pursuant to article 39 paragraph 1 letter a) of the GDPR. In the event that an operator realizes that such problems are necessary for an operator of another LEA involved in the project, within the limits of sustainable effort, it will be the operator's responsibility to inform his/her colleagues of the presence of legal and ethical problems and to take action together with him/her in contacting the DPO.[3] In the Exploitation Phase, the LEAs involved shall strictly comply with the criminal procedure codes of their country.

---

[1] For example, Dermot Feenan reports his study of paramilitary violence in Northern Ireland in which operators needed to become accepted as part of a paramilitary group, with the danger that they might have to become involved in illegal activities. Feenan has shown that in such cases ethical and legal consultation is essential to define a shared course of action (*Justice in conflict: Paramilitary punishment in Ireland (North)*, in *International Journal of the Sociology of Law*, 30(2), pp. 151-172, June 2002).

[2] An EU Code for Ethics for socio economic research - Sally Dench Ron Iphoen Ursula Huws – IES, GB.

[3] Article 39, Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing,

1.2 Discrimination

In the Research Phase, ANITA shall have a common preliminary knowledge base. In the second phase, LEAs shall host on-premises their ANITA instance, the knowledge base of which they shall update on their own.

Concerning the Research Phase, ANITA's project commitments shall ensure that:

a) In contributing to the design of ANITA, LEAs' operators shall pay attention to, and respect, all groups, regardless of their race, ethnicity, religion or culture. A key issue is the use of racist or xenophobic annotations in the Research Phase and the basing of research on stereotypes of different racial, ethnic, religious and cultural groups. LEAs' operators and ANITA consortium partners shall collaborate in the tool developing phase, which take into account how they conduct investigations and what is considered relevant by them, in a responsible way because the wording used may impact the ANITA deployment.

b) During the Research Phase, when taking annotations of videos and images with information that the LEAs consider relevant, LEAs' operators shall be instructed not to include discriminatory content or content that may be outside the context of ANITA. This requirement shall be strictly respected because ANITA, once finished, will automatically act according to the parameters that at this stage, the LEAs have established through such annotations. In this phase, the LEAs are therefore committed to working together in order not to use discriminatory annotations in the process of annotation of images and videos that serves for the training of ANITA. ANITA is a tool based on powerful machine learning algorithms and datasets actually collected in the most populated illegal markets of the darkweb, which makes ANITA a powerful tool and therefore, in the phase of creating the necessary keywords, LEAs' operators must collaborate in order to find common points in their needs. In this sense, the collaboration of the LEAs will be necessary to identify the most correct terminologies and images in order to create the most effective dataset in the training of the tool.

c) The purpose is to encourage a general sensitivity to the ways in which racist terminology may be perceived and used by the LEAs' operators. The main goal of the project is to develop a tool that benefits society and minimizes social harm. This means that any benefits arising during the Research phase shall not cause any harm or prejudice and shall not go beyond the objectives that the Consortium has set in the Grant Agreement. This does not mean that the system shall not perform above the specified level, but that the algorithm shall not be trained in a way which has discriminatory effect. Research, or the tool itself, may cause harm, for example, to a particular group in society due to the possible misuse in the training process or in the use of the tool. This is perhaps particularly relevant to groups related to UC3 which is related to terrorism. A balance that has to be made is when the usage of ANITA might lead to findings that are negative or disadvantageous to one particular group, but that contribute to the overall greater good in society. In this regard, the LEAs will have to collaborate in order to carefully select the wording necessary for the training of the machine learning algorithm that is the basis of ANITA and will have to avoid

---

including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

using words that could lead to a mismatch in the logic of the tool, losing the purpose of identifying cyber criminals.

d) Discriminatory annotations are those based on special categories of personal data according to article 9 paragraph 1 of the GDPR[4], such as faith. Therefore, the LEAs undertake to use annotations that are not relevant only because they derive from the faith or political and philosophical beliefs of individuals but that, in connection with the experience of the LEAs themselves, may contain additional elements. During the Research Phase of the ANITA Project, personal data can be

[4] Article 9, Processing of special categories of personal data
1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

collected from the (dark, deep, surface) web using specific tools. These data are normally from sources freely accessible by anyone and may also potentially belong to the special categories referred to in Art. 9(1) GDPR. This issue has been analysed in Deliverable 3.4 Data Protection Office. Tools like ANITA can be exploited either for social good or be misused. The professionalism encouraged by this collaboration policy is based on their use in socially responsible pursuits by morally responsible operators.

1.3 Data Protection

ANITA project takes into great consideration the compliance to personal data protection principles set out by GDPR and by Directive 2016/680. Therefore, ANITA's project commitments will be able to ensure that, in any step of the project, shall be grant that personal data will be:

1) processed lawfully, fairly and in a transparent manner in relation to the data subjects (*'lawfulness, fairness and transparency'*);
2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compliant with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (*'purpose limitation'*);
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*'data minimization*');
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*'accuracy'*);
5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures in order to safeguard the rights and freedoms of the data subject (*'storage limitation*');
6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (*'integrity and confidentiality'*).

1.3.1 The Research Phase

a) Even if used by LEAs, ANITA tool in the Research Phase is not used for generic law enforcement purposes, nor for the specific purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This means that Directive 2016/680/UE and national implementing laws shall not apply to this phase, while GDPR rules applies to processing of personal data in the Research Phase.

b) ANITA will mainly collect publicly available data, from the (dark, deep, surface) web. In this case, we have to take into account the following points:

> Collecting data from the web (dark, deep, surface) could imply also personal data collection.

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

> The possibility that an information can be considered as "personal" according to the GDPR is, then, very likely to occur, since the identifiability could derive not only from direct identifier that could be deleted or not collected (so called "K-anonymity") but also through the combination of many other elements (so called "L-diversity").

> Data are going to be collected from sources that are different from the data subject; that is, data are not obtained directly from the data subject him/herself, but from websites and other third online publicly available parties. In these cases, we can also assume that the users generated contents made (at least, if any) their own data/metadata manifestly public, even if trying masking and anonymizing their navigation identity, once they uploaded and/or shared online visible content.

> In case of third data subjects, to whom a specific content could refer, who are different from the users generated contents, we can *a fortiori* assume that such data would not be obtained from the data subject but from other sources. In this case, the only difference would be that their (third data subjects different from the uploading/sharing users) data would not be voluntarily and manifestly made public by themselves.

c) The collection and the further processing of personal data for scientific research and/or statistical purposes (within a H2020 project like ANITA, that is regulated by the European Union and national laws), shall be conducted according to the following principles:
   - The respect of principles set by articles 5 and 25 of the GDPR.
   - The presence of legal grounds for data processing according to articles 6-9-10-89 of the GDPR.
   - The obligation to inform data subjects (or its exceptional exclusion) according to articles 13-14 GDPR.

1.3.1.1 The respect of principles set by Articles 5 and 25 of the GDPR

a) LEA's operators for the collection and the further processing of personal data for scientific research and/or statistical purposes shall respect the following general principles:

I. processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency');**

II. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');**

III. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation');**

IV. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy');**

V. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**; personal data may be stored for**

longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');

VI. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality').**

b) **LEAs, developers, technical partners and all subject involved in the design phase, shall respect data protection by design and by default principles** taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **they shall, during the project, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects**.

c) Apart from the technical and organisational measures implemented in ANITA by the technical partners of the project, LEAs shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

d) It is clear that also the selection of types of data, at the moment of the collection, and the choice of kinds of means and modalities of data processing can affect the principles-related aspect. If one collects more personal data and of types and for processing activities that are useless for the purposes/objectives of the research project, then, this would result in a breach of law. Notwithstanding this, it is true that big data mining and AI applications could more and more conflict, potentially, with these principles, particularly at the moment of collection and early processing.

1.3.1.2 The presence of legal grounds for data processing according to Articles 6-9-10-89 of the GDPR

Respecting fundamental principles is not enough. A scientific research project shall find one or more legal grounds (legitimate basis) for data processing. This could be found, in general, within the GDPR, precisely in the articles 6, 9, 10 and 89: these are the relevant norms in matter of legal grounds for scientific research and/or statistical purposes of data processing.

Article 6 provides the basic grounds for personal data processing. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In bold you can read the main legal grounds that could be referred to a processing activity for scientific research and/or statistical purposes.

In case of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), **article 9, paragraph 2 letters e), g), j) potentially apply to the processing for scientific research and/or statistical purposes, providing that such processing is not prohibited if**:

(e) processing relates to personal data which are manifestly made public by the data subject;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(j) processing is necessary for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes** in accordance with article 89 paragraph 1 based on Union or Member State law which **shall be proportionate to the aim pursued**, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

These lawfulness conditions in case of special categories of data have to be added to the possible legal grounds set by article 6 of the GDPR, even if the conditions under letters g) and j) could be considered as inclusive of legal grounds already set by article 6, while processing related to personal data which are manifestly made public by the data subject should be linked to another legal ground (for instance, just the legitimate interest of the data controller or the processing in the public interest).

The above listed legal grounds and lawfulness conditions are general, at the European Union level (that is the scope of the GDPR), but it can happen that single States add and require for further conditions in order to enable scientific research without data subject's consent (remember that data subjects' consent is just another legal ground which could legitimate a processing activity). For instance, in Italy, according to article 110 of the national Privacy Code, clinical/health scientific research studies require additional conditions to be fulfilled, in order to process special categories of data without the data subject's consent.

In case of re-use in the Research Phase of personal data that were collected before, while acting as LEAs for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, article 9 of the Directive 2016/680/UE applies:

Article 9

Specific processing conditions

1. *Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.*
2. ***Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.***
3. *Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.*
4. *Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.*

This means that, at least **in the case of reuse for scientific research or statistical purposes, the GDPR should apply as well, in the Research Phase, but there could be specific limitations to the reuse of specific data provided by national laws (e.g. data coming from interceptions, investigations, etc.).** If no limitations are provided by national laws to LEAs' data reuse for scientific purposes, data reuse can be done, respecting GDPR and national supplementing laws protecting personal data.

1.3.1.3 The obligation to inform data subjects (or its exceptional exclusion) according to Articles 13-14 GDPR

To respect general fundamental principles and to ensure a valid legal grounds/lawfulness conditions of data processing could not be enough. A general rule, coming from articles 13 and 14 of the GDPR, **imposes to adequately inform data subjects** about their personal data processing. This is the "privacy notice" or "privacy policy" that we are used to receive as data subjects and users, almost in all cases our data are going to be collected and processed (some exceptions occur, for instance, just in justice/law enforcement scenarios).

Collecting data from the (dark, deep, surface) web, such as collecting data from publicly available records and documents, implies that data are not obtained directly from the data subject. **In this case (collection not from the data subject, but from third parties), article 14.5.b) of the GDPR applies and justify at certain conditions even the exclusion of the obligation for the data controller to inform data subjects, where and insofar as "*the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available*."**

It seems reasonable that Use Cases in ANITA Project all refer to scenarios in which "*the provision of such information proves impossible or would involve a disproportionate effort".* **This could permit to exclude the**

obligation to inform, for data controllers involved in ANITA Project, but it would persist an obligation to publish the information and to make it publicly available (e.g. on the website).

Single States, nonetheless, could require for additional authorisations in order to lawfully process personal data for scientific research and/or statistical purposes without information to data subjects. For instance, in Italy it is mandatory for Italian data controllers (researchers), according to article 110-bis of the Privacy Code, to obtain a prior authorisation from the Italian Data Protection Authority, in case the further processing of data is being carried out by a third party – that means another data controller different from the first one that collected/processed the data before. This could apply also to ANITA scenarios, in case dataset collected by different Partners will be shared between and with other Partners involved in the project.

1.3.2 The Exploitation Phase

Personal data processing in the exploitation phase will be reasonably carried out by LEAs, using ANITA's tools, for law enforcement purposes, including prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This will imply the application of Directive 2016/680/UE and related implementing laws, in addition to all the national laws and rules in matter of criminal procedure, public security, national security, etc. It will be necessary to check every single national law, as applicable to the Use Case(s), in order to address possible limitations and lawfulness conditions for such data processing.

1.3.3 Checklist

Prior Key Questions checklist in order to process data for scientific research and/or statistical purposes

1. Is the (personal) dataset originally collected from publicly available sources and then processed by the data controller for scientific research and/or statistical purposes? **IF YES, PERSONAL DATA PROCESSING ACTIVITIES HAVE A VALID LEGAL GROUND AND RESPECT THE PURPOSE LIMITATION PRINCIPLE. IF YES, SKIP TO QUESTION NO. 7.**
2. Was the dataset originally collected from private physical or virtual environments* (e.g. contents in a social network account, not made manifestly public by the user, obtained becoming "friend" of him/her) and then processed by the data controller for scientific research and/or statistical purposes? **IF YES, CHECK THE APPLICABLE NATIONAL LAW AND SOCIAL NETWORK TERMS & CONDITIONS FOR POSSIBLE LIMITATIONS TO SUCH DATA COLLECTION AND REUSE.** **Please take into account that national constitutions and laws could prohibit data collection and reuse, even for scientific research and/or statistical purposes in other cases and fields.*
3. Was the dataset originally and lawfully produced/collected/processed by LEAs only for the purposes of law enforcement, justice, prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and now is it going to be processed by the same data controller for scientific research and/or statistical purposes? **IF YES, CHECK THE APPLICABLE NATIONAL LAW FOR POSSIBLE LIMITATIONS TO SUCH DATA REUSE.**
4. Was the dataset originally and lawfully produced/collected/processed by a data controller only for the purposes of providing a communication service, and now is it going to be processed by the same data controller for scientific research and/or statistical purposes? **IF YES, CHECK THE APPLICABLE NATIONAL LAW FOR POSSIBLE LIMITATIONS TO SUCH DATA REUSE.**
5. Was the dataset originally and lawfully produced/collected/processed by a data controller only for the purposes of a clinical/health study, and now is it going to be processed by the same data controller for other non-clinical/health scientific research and/or statistical purposes (e.g. ANITA

Project)? **IF YES, CHECK THE APPLICABLE NATIONAL LAW FOR POSSIBLE LIMITATIONS TO SUCH DATA REUSE.**

6. Was the dataset originally and lawfully produced/collected/processed by the data controller for purposes other purposes (but different from the purpose of providing a communication service, from the purposes of clinical/health scientific research and from purposes of law enforcement, justice, prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties), and now is it going to be processed by the same data controller for scientific research and/or statistical purposes? **IF YES, PERSONAL DATA PROCESSING ACTIVITIES HAVE A VALID LEGAL GROUND AND RESPECT THE PURPOSE LIMITATION PRINCIPLE. IF YES, GO TO NEXT QUESTION NO. 7.**
7. Are the dataset collection (in terms of quality and quantity of data) and the related processing activity respecting the general principles according to articles 5-25 of the GDPR (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, proportionality, storage limitation, integrity, confidentiality, data protection by design & by default)? **IF YES, PERSONAL DATA PROCESSING IS COMPLIANT WITH GENERAL PRINCIPLES. GO TO NEXT QUESTION NO. 8.**
8. Is the provision of privacy notice/information to data subjects impossible or would it involve a disproportionate effort, in particular for processing (carried out by the same data controller that originally collected data) for scientific research purposes or statistical purposes, or is it likely to render impossible or seriously impair the achievement of the objectives of that processing? **IF YES, THE PROCESSING IS LAWFUL BUT THE DATA CONTROLLER SHALL TAKE APPROPRIATE MEASURES TO PROTECT THE DATA SUBJECT'S RIGHTS AND FREEDOMS AND LEGITIMATE INTERESTS, INCLUDING MAKING THE INFORMATION PUBLICLY AVAILABLE.**
9. Is the provision of privacy notice/information to data subjects impossible or would it involve a disproportionate effort, in particular for further processing (carried out by third parties, such as another data controller different from the controller that originally collected the dataset) for scientific research purposes or statistical purposes, or is it likely to render impossible or seriously impair the achievement of the objectives of that processing? **IF YES, CHECK THE APPLICABLE NATIONAL LAW FOR POSSIBLE LIMITATIONS TO SUCH DATA REUSE BY THIRD PARTIES.**

2 Cooperation in Incident Handling

In order to maintain the confidentiality, availability and integrity of the data and information relating to the investigations and to establish a network of internal collaboration between ANITA users within the LEAs, it is necessary to follow the provisions set forth in this policy.

The objective of establishing a level of cooperation on security incidents is to ensure that the collaboration between LEAs from different countries can guarantee a mutual protection regime that designs a safety framework for all those who work on the tool.

To this purpose, it is necessary to ensure the security of networks and systems, understood as the ability of a network and information systems to resist, at a certain level of confidentiality, any action that compromises the availability, authenticity, integrity or confidentiality of the data stored or transmitted or processed and the related services offered or accessible through that network or information systems. The purpose of ensuring security implies a process of collaboration between the LEAs in relation to all security events, i.e. an observable event in a system or network consisting of an observable change in the usual behaviour of a system or process.

LEAs, developers and technicians will therefore cooperate in order to distinguish false positives from actual security incidents. The false positive is a false alarm i.e. it is the event that is not real or that does not even potentially materialize as a negative because it has no consequences (e.g. the fire alarm sounds even if no fire is in progress, or the alarm at the entrance door of a data centre that actually remains closed, etc.); in the IT environment, it is a legitimate program detected as dangerous by a security program (an example in IT is an antivirus that mistakenly considers a harmless program to be harmful or despite the alert no hacker attack has occurred).

The purpose of this policy is to avoid and manage, in a collaborative manner within the network of LEAs using ANITA, the Incident, intended as any event with a real prejudicial effect on the security of the network and information systems, a violation or imminent threat of violation of security policies and lawful use of technological tools, also intended as an Event that produces negative effects on the confidentiality, integrity or availability of data within the LEAs and/or that negatively impacts on the processes of the LEAs.

LEAs will have the possibility, through the tool, to collaborate effectively in reporting the Event. Specific functionalities will be made available within the software in such a way as to be able to report any faults, malfunctions or bugs that have not been catalogued as security incidents, thus allowing the operators of the LEAs involved to correct any incorrect behaviour or to avoid the above mentioned cases.

The information collected together with the determination of the incident classification is reported in the Event Sheet (attached to this procedure) and possibly further detailed and documented, together with the work carried out in the other steps, in a special report.

If the determination reached is that the Event cannot be considered an Incident, the procedure is terminated.

If this is not the case, the LEA that found the Incident will proceed to report it to the operators of the LEAs, classifying it according to the table below. In particular, the type of Incident is assessed by drawing on consolidated international classifications. The following one, in Table 1, is based on the taxonomy of the "European CSIRT Network" (eCSIRT)[5].

Category	Example subcategory	Description	Low Level	Medium Level	High Level
Unauthorized access	**Compromised account**	The account is compromised.	A single user account is compromised by the source of the threat.	More than a single account of more than a single user is compromised by the source of the threat.	An account that can access a considerable amount of personal or confidential data is compromised with proven data loss.
	Generic Unauthorized Access	Unauthorized access to systems, hardware, software.	Unapproved access that did not cause damage to resources.	Unapproved access that has caused moderate damage to the resources.	Unapproved access that has damaged services or processes defined as critical or potentially compromised Personal Data.
	Phishing	Attempted scam aimed at grabbing confidential information on a large scale.	The user or resource concerned does not deal with personal data or confidential information.	The user or the resource concerned has the potential to establish a compromise of personal data or confidential information.	The user or resource concerned has accessed an external link or opened an attachment sent via the phishing e-mail and/or performed the action requested by the attacker.
	Scan	Scanning the network,	Reconnaissance attempts have a	Attempts to reconnaissance	Reconnaissance attempts result in

[5] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Category	Example subcategory	Description	Low Level	Medium Level	High Level
		systems, processes presumably by an attacker.	minimal impact on resources.	are carried out on systems considered vulnerable and/or affect the functionality of resources.	an attack.
	Spear Phishing	Attempt to defraud people whose behaviour has previously been the victim of a special study in order to obtain specific information.	The text of the communication does not contain any information other than contact information, which is public.	The text of the communication contains non-public contact information and non-public hierarchical references.	The text of the communication simulates previous ones, contextualizing roles and responsibilities and conveying non-public information.
Abuse	**Disclosure**	Dissemination of information outside the perimeter of the organization.	Unauthorised disclosure of confidential information has certainly not taken place.	Unauthorised disclosure of confidential information has not been established.	Unauthorised disclosure of confidential information has occurred.
	Mis-configuration	Error in the configuration of a system, hardware, software.	Authentication and/or Authorizations configured with minimal impact on resources.	Authentication and/or Authorizations configured incorrectly with a moderate impact on resources.	Wrongly configured authentication and/or authorizations with a strong impact on resources.
	Misuse	Error using a system, hardware, software.	The error has a minimal impact on resources.	The error has a moderate impact on resources.	The mistake has a serious impact on resources.
	Policy and/or Procedure Violation	Violation of policies and procedures established by	Violation of the Policy/Procedure has a low impact.	Violation of the Policy/Procedure has a moderate impact.	Violation of the Policy/Procedure has a serious impact.

Category	Example subcategory	Description	Low Level	Medium Level	High Level
		the organization.			
	Theft	Hardware theft.	The stolen hardware has a low monetary value and is not part of a system defined critical.	The stolen hardware has a high monetary value or is part of a critical system.	The incident investigation is the related response to it shall be transferred to the competent authorities.
Denial of Service	**Business Impact**	Impact on the organisation's core/critical systems.	The incident does not involve critical services.	The incident involves critical services.	The incident involves critical services and threatens to involve more.
	DDoS	Deliberate exhaustion of the resources of a computer system that provides a service, such as a website, to the point where it is no longer able to provide the service itself.	The resources concerned are not defined as critical.	The resources concerned have moderate impact on production/critical systems.	The resources concerned have a serious impact on production/critical systems.
	Loss	Loss of hardware.	Lost hardware has a low monetary value or is not part of a system defined critical.	Lost hardware has a high monetary value or is part of a critical system.	The incident investigation and its response shall be transferred to the competent authorities.
	Service disruption	Interruption of service.	The incident concerns a single resource and/or a single endpoint.	The incident affects more resources and more endpoints, compromising	An interruption of service defined as critical occurs.

Category	Example subcategory	Description	Low Level	Medium Level	High Level
				services.	
Malware	**Generic Malware**	A program or file that can damage computers and systems.	A single endpoint is infected.	Several endpoints are infected.	Infection actively spread; the impact affects several areas of the organization.
	Ransomware	Type of Malware that restricts access to the device that infects the data it contains, requiring a ransom to be paid to remove this limitation.	The resource has been infected but has been prevented it from spreading.	The resource is infected and spreads to a small number of other resources.	The resource is infected, and this has a serious impact on the entire organization.
	Zero-day	The exploitation of a vulnerability not expressly known to the software developer.	Minimal impact on resources.	Moderate impact on resources.	Strong impact on resources.

In certain circumstances detailed below, when the Event or Security Incident involves personal data of operators or any directly or indirectly identifiable natural person, in order to protect the identity of operators and in order to safeguard the LEAs network involved in the use of the tool, it will be necessary for LEAs to cooperate in order to report and manage Personal Data Breach cases.

2.1 Personal Data Breach: gathering of information

This paragraph applies also to the Research Phase and is dedicated to the management of personal data breaches to facilitate cooperation between LEAs. The instructions below have therefore been developed to establish a universal framework for incident management procedures and for defining roles and responsibilities while ensuring guarantees towards the parties concerned and the operators themselves. After the first phase of evaluation of the information collected, the proposed discipline is substantiated in the eventual notification to the competent authority and in the communication to the interested subjects if the destruction, loss, modification, unauthorized disclosure or access to data personal data transmitted, stored or in any case processed may have negative consequences for the interested parties and the operators themselves. Unless otherwise provided herein, all the terms in capital letters in this document

refer to definitions included in the GDPR and are reported for convenience in the “Definitions, Acronyms and Abbreviations” section.

2.2 Phase 1: gathering of information

2.2.1 Internal Channels

Internal reports regarding abnormal events may:

- be sent by LEAs operators or ANITA's partners;
- be forwarded by the DPO.

2.2.2 External Channels

These reports may also be received from external sources, e.g., from the ANITA's website, from the ANITA's social media pages (e.g., Facebook, Twitter, etc.).
Data Subjects may also report that their Personal Data have been misused or fraudulently processed by a Third Party, even if they merely suspect this to be the case; whenever they choose to do so, Data Subjects may request that the ANITA project check if any such misuse or unlawful processing occurred.
All reports, made to any subject or function within the ANITA project, must be promptly communicated to the Data Breach Assessment and Management Unit ("DBAMU"), which will be composed of the following functions / persons: DPO and Project Coordinator or his/her delegate, in any case no later than 24 hours from the moment on which any subject or function becomes aware of a Personal Data Breach. The DBAMU is in charge of all Personal Data Breach reports and will manage them.

2.3 Phase 2: Analysis

2.3.1 Preliminary Analysis and Elaboration of the Event Sheet

The DBAMU will first begin a preliminary analysis, aimed at collecting information on the abnormal event occurred and compiling the Event Sheet (see Annex A to this Policy) with all details collected:

- Date on which the abnormal event occurred;
- Date on which the Personal Data Breach is presumed to have occurred;
- Date and time on which the ANITA project became aware of the Personal Data Breach;
- Source which reported the Personal Data Breach;
- Type of Personal Data Breach and categories of Personal Data affected;
- Description of the abnormal event;
- Number of affected Data Subjects;
- Number of Personal Data records which are presumed to have been breached;
- Place where the Personal Data Breach occurred;
- Brief description of the Personal Data processing or storage systems affected, as well as their location.

The Event Sheet will then be sent for first-level analysis, as described below.

2.3.2 First-Level Analysis – Warning Assessment

The first-level analysis' goal is to verify that a report received is not a "false positive".
If it is confirmed that a Personal Data Breach actually took place, the DBAMU, which is in charge of the first-level analysis, will (with the collaboration of LEAs or partners affected by the Personal Data Breach) retrieve any detailed information on the Personal Data Breach which may be necessary for the second-level analysis and include this in the Event Sheet.
If the reported event turns out to be a false positive, the incident will be closed. The event will then be logged in the "false positive events" section of the Register of Personal Data Breaches by the DPO (see Annex C to this Policy).

2.3.3 Second-Level Analysis – Personal Data Breach Sheet

The Data Breach Assessment and Management Unit ("DBAMU") is also in charge of the second-level analysis.
The DBAMU will jointly analyse all information collected and draw up a Personal Data Breach Sheet (see Annex B to this Policy) for the resulting assessments.
The DBAMU will classify an analysed event according to the following categories:

- Unlawful destruction of Personal Data;
- Unlawful loss of Personal Data;
- Unlawful modification of Personal Data;
- Accidental destruction of Personal Data;
- Accidental loss of Personal Data;
- Accidental modification of Personal Data;
- Unauthorised disclosure of Personal Data;
- Unlawful access to Personal Data.

The Personal Data Breach must then be assessed according to the following risk levels:

- NONE
- LOW
- MEDIUM
- HIGH

These risk levels refer to the probability that one of the following adverse effects may occur, to the detriment of natural persons (even if those persons are not affected Data Subjects), as a result of the Personal Data Breach:

1. Discrimination;
2. Identity theft or fraud;
3. Financial loss;
4. Damage to reputation;
5. Loss of confidentiality of personal data protected by professional secrecy;
6. Unauthorised reversal of Pseudonymisation;
7. Significant economic or social disadvantage;
8. Deprivation or limitation of rights and/or freedoms;
9. Loss of control over Personal Data;
10. Other physical, material or non-material damage to natural persons.

The following possible circumstances must also be assessed, as qualitative variables affecting the potential impact of a Personal Data Breach:

a) Whether the affected Personal Data reveal Data Subjects' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or include genetic data, health data or data relating to sex life, criminal convictions and crimes or related security measures regarding Data Subjects;
b) Whether the affected Personal Data was being used in the assessment of certain personal aspects relating to Data Subjects, in particular to analyse or predict aspects concerning those Data Subjects' performance at work, economic situation, health, personal preferences, interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
c) If the affected Personal Data relates to vulnerable natural persons, in particular to minors;
d) If the Personal Data Breach affected a significant amount of Personal Data records;
e) If the Personal Data Breach affected a large number of Data Subjects.

The DBAMU must, in any case, ensure that measures to minimise the potential adverse effects of the Personal Data Breach are taken promptly.

2.4 Phase 3: Notifications and communications

2.4.1 Notification to the competent Data Protection Authority

1) Having drafted the Personal Data Breach Sheet, the DBAMU must then assess actions to be taken, as well as begin the process to notify the competent Data Protection Authority and, where necessary, communicate information on the Personal Data Breach to the affected Data Subjects. This will be done by verifying and validating documentation received during the previous phases of work.

2) The DPO will be in charge of notifying the Personal Data Breach to the competent Data Protection Authority without undue delay and, where possible, within 72 hours from the moment on which the ANITA project became aware of the existence of the Personal Data Breach in question. Only where a Personal Data Breach is unlikely to present a risk to the rights and freedoms of individuals and, therefore, has had its risk level classified as "NONE" (see Section III(C) above), does this notification not need to be carried out.
3) Where mandatory, if the notification to the Data Protection Authority is not made within 72 hours, it must be accompanied by the reasons for the delay.
4) All notifications to the Data Protection Authority must:
    a) Describe, to the extent possible:
        i. the nature of the Personal Data Breach;
        ii. the categories and the approximate number of Data Subjects involved;
        iii. the categories and the approximate number of Personal Data records involved;
    b) Include the name and contact details of the DPO, or of another contact point where more information on the Personal Data Breach can be obtained;
    c) Describe the likely consequences of the Personal Data Breach;
    d) Describe the measures taken, or proposed to be taken, by the ANITA project to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
5) Where, and in so far as, it is not possible to provide all the above information at once, it may be provided in phases as it becomes available, without undue further delay.

2.4.2 Communication to Affected Data Subjects

Whenever the DBAMU, under articles 33 and 34 GDPR, assesses that a Personal Data Breach's potential risks to the rights and freedoms of natural persons must be classified as "HIGH" in the Personal Data Breach Sheet (see Annex B to this Policy), the DPO must inform the Data Subjects regarding that Personal Data Breach.
In these cases, information on the Personal Data Breach must be communicated to affected Data Subjects without undue delay, as soon as the Personal Data Breach has been acknowledged and properly assessed, through the channels deemed most appropriate by the DBAMU. The communication must be intelligible, concise, transparent and easily accessible to Data Subjects, using clear and plain language - wherever possible, the communication is to be drafted in the language spoken by the affected Data Subjects.
Any communication regarding a Personal Data Breach to affected Data Subjects must contain the following information:

a) Date and time on which the Personal Data Breach occurred, or is presumed to have occurred, as well as date and time on which the ANITA project became aware of the Personal Data Breach;
b) A description of the nature of the Personal Data Breach;
c) The name and contact details of the DPO;
d) A description of the likely consequences of the Personal Data Breach;
e) A description of the measures taken, or proposed to be taken, by the ANITA project to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

It is not necessary to communicate information on a Personal Data Breach to Data Subjects if one of the following conditions has been met:

a) Appropriate technical and organisational protection measures have been implemented and applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access this Personal Data, such as encryption – this will not apply, however, where the Personal Data Breach results in the destruction or loss of that Personal Data;
b) Subsequent measures have been taken, ensuring that the high risk to the rights and freedoms of natural persons, as assessed, is no longer likely to materialise – in this case, these measures must be documented in the Register of Personal Data Breaches;
c) The communication would involve a disproportionate effort – in this case, there must instead be a public communication or similar measure taken whereby the Data Subjects are informed in an equally effective manner.

A template for communication of a Personal Data Breach to affected Data Subjects is provided at the end of this Policy (see Annex D to this Policy).

2.5 Phase 4: Recording in the register of personal data breach

The DBAMU is to document every single abnormal event which it analyses in the Register of Personal Data Breaches (see Annex C to this Policy), regardless of whether the event is assessed as FALSE, IRRELEVANT or RELEVANT.
Regarding IRRELEVANT and RELEVANT events, the following information must be logged in the Register:

- Actual or potential consequences of the Personal Data Breach;
- Measures taken to remedy or mitigate those consequences;
- Notifications made to the Supervisory Authority;
- Communications made to Data Subjects.

This documentation will allow the Data Protection Authority to verify the ANITA's project compliance with the rules on Personal Data Breach notification and communication.
The Register of Personal Data Breaches is maintained by the DPO under the responsibility of Project Coordinator.

2.6 Phase 5: post-breach analysis

The last stage of the Personal Data Breach management process is to carry out a final collection of evidence and any additional information gathered regarding the detected Personal Data Breach, and to assess this evidence and information, in order to perform a post-breach analysis.
The aim of this analysis is to confirm the effectiveness and efficiency of actions taken during the management of the Personal Data Breach and to identify possible areas for improvement.

3 Cooperation with Data Protection Authority

This Procedure aims to provide operating instructions that the LEAs part of the ANITA Consortium has put in place in order to deal with inquiries, information requests and inspections (hereinafter, the "**Inspections**") carried out by a Data Protection Authority.

Unless otherwise provided therein, all the terms in capital letters in this document refer to definitions included in the GDPR and are reported for convenience in the "Glossary and Acronyms" section.

3.1 Communication Obligations

According to articles 31 and 39 paragraph 1 lett. d) of the Regulation, the ANITA project delegates the task of cooperation and communication with a Data Protection Authority to the DPO.

3.2 Obligations of Natural Intervention, Cooperation and contact

In line with the commitments undertaken by the ANITA project pursuant to articles 31 and 39 paragraph 1 lett. (d of the Regulation, the DPO shall be promptly and adequately involved in all matters that relate to the protection of personal data concerning both the special obligations, as in the event of Inspections; but also the natural intervention, cooperation and contact obligations under the Policy on Data Breach Management part of this policy.

3.3 Consultation Obligations

According to articles 36 and 39, paragraph 1, letters d) and e) of the Regulation, the ANITA project delegates the obligations of prior consultation as a result of residual risks that may arise from the Procedure on Data Protection Impact Assessments and, where appropriate, consultations concerning any other subject, to the DPO.

In this respect, the DPO is required to get in touch with a Data Protection Authority and to provide all necessary information to fulfil the obligations and the time limits laid down in the Regulation.

Pursuant to Article 39, paragraph 1, letter d) of the Regulation, the obligation to cooperate with the Data Protection Authority, during the Inspections, concern the DPO and LEAs' operators that are physically present at the arrival of a Data Protection Authority and/or its representatives.

The Inspections shall be carried out in phases and with the procedures below.

3.4 Phase 1: access and request for information

In the event of an Inspection at the premises of a LEA involved in the ANITA project, the operator that is physically present at the arrival of a Data Protection Authority and/or its representatives, shall immediately warn the DPO appointed by the LEA, who shall verify both the identity of a Data Protection Authority and the purpose of its visit in order to determine the subject-matter of the Inspection, and, if the matter of inspection regards, even indirectly, ANITA, the ANITA's project DPO has to be warned.

The DPO provides all necessary instructions to the LEAs' operators who were present when a Data Protection Authority and/or its representatives arrived, and determines which actions has to be taken and which people to eventually involve in the Inspection Unit, which is a Unit composed by the DPO of the LEA, if appointed or its privacy contact if not appointed, and the DPO of the ANITA project.

3.5 Phase 2: Verification and Response

In this phase, the Inspection Unit has the task of assisting a Data Protection Authority and/or its representatives in verifying compliance with the Regulation and other applicable laws.

The DPO provides for the information requested by or on behalf of the Data Protection Authority.

Save for exceptional cases or particular requests for information by a Data Protection Authority and/or its representatives, the Inspection Unit should not provide any further details than those already stated in the Grant Agreement of the ANITA project.

The DPO, or the Inspection Unit, shall pay particular attention to the assessment of any information that is additional to or different from the one contained in the Grant Agreement.

As a general rule, it is important that the Inspection Unit always remembers the following instructions:

- keep a friendly and cooperative attitude;
- ask a Data Protection Authority and/or its representatives, in case of unclear requests for information, for further details and clarifications before answering or handing out documents.

3.6 Phase 3: conclusion

This phase consists in the drafting of the final report on the verification activities, which reflects the outcome of the Inspection by the Data Protection Authority.

This report is an important document, as it records the entire inspection activity to indicate the seized documents and the statements of the ANITA project.

Before signing the report, the DPO, or the Inspection Unit, shall attentively read the text and verify whether the facts stated therein are consistent with the order of the events of the Inspection.

If that is the case, the DPO signs the report and requests for a copy of the signed report.

The report should, in general terms, contain the following information:

- date and place of the Inspection;
- identification details and function of the person writing the report;
- identification details of the inspected LEA as partner of the ANITA project;

- seized files and documentation;
- requests and respective responses / answers given by the LEA as part of the ANITA project;
- statements of the DPO/Inspection Unit;
- detailed descriptions of any fact constituting of a violation;
- any provisions violated and the relevant seized evidence;
- signature of the subject who wrote the report and of the representative of the inspected LEA as partner of the ANITA project.

4 Cooperation in the usage of ANITA

In order to establish a successful collaboration between LEAs, allowing LEAs' operators to cooperate using the tools of ANITA, in the exploitation phase, with all its potential but with maximum security, it is necessary that LEAs shall respect the rules contained in this policy, enforcing them within their departments and systems.

In this regard, it is necessary to equip ANITA to better support Member States in a Union-wide crime prevention, analyses and investigations. To achieve this goal, LEAs need to cooperate more closely following the principles of the EU legal framework. In this context, according to the rules set forth by Chapter III of the Budapest Convention on Cybercrime of 23rd November 2001, LEAs shall co-operate with each other, to the widest possible extent for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence. Also, the provisions of the Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation – "**Europol**" (hereinafter "**Europol Regulation**"), in particular those concerning cooperation, shall address the LEAs' collaboration.

ANITA should be a hub for information exchange between LEAs: this is one of the principles of cooperation set forth in this policy. Of course, each LEA may implement the tool according to its needs and national law. Information collected, stored, processed, analysed and exchanged by LEAs include criminal intelligence which relates to information about crime or criminal activities falling within the scope of ANITA's objectives, obtained with a view to establishing whether concrete criminal acts have been committed or their possible trends in the future.

In order to ensure the effectiveness of ANITA as a hub for the information exchange, clear obligations should be laid down requiring LEAs to provide ANITA with the data necessary for it to fulfil its objectives, as set forth in this policy. While implementing such obligations, LEAs should pay particular attention to provide data relevant to the fight against crimes for which ANITA tool is developed.

To enhance the usability and efficiency of the tool and to increase operational cooperation between the LEAs, and particularly to establish links between data already in the possession of the different agencies, ANITA could enable Eurojust, Europol and the European Anti-Fraud Office (OLAF) to have access, on the basis of a hit/no hit system, to data available at ANITA. Any access to data available at ANITA should be limited, by technical means, to information falling within the scope of the Project according to this Policy's rules.

Data protection rules in the ANITA project should be strengthened and be drawn on the principles underpinning Regulation (EU) 2018/1725 to ensure a high level of protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and EU national agencies and to the free movement of such data. As Declaration No 21[6] recognises the specificity of personal data processing in the law enforcement context, the data protection rules applicable to ANITA should be also consistent with other relevant data protection instruments applicable in the area of police cooperation in

[6] The Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation is attached to the TEU and TFEU. Document 12007L/AFI/DCL/21. *Official Journal 306, 17/12/2007 P. 0257 – 0257*.

the European Union. Those instruments include, in particular, Directive (EU) 2016/680 of the European Parliament and of the Council, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Recommendation No R(87) 15.

Member States should also endeavour to provide LEAs with a copy of bilateral and multilateral exchanges of information with other Member States on crime falling within ANITA's objectives. At the same time, LEAs should increase the level of their support to Member States, so as to enhance mutual cooperation and the sharing of information through the use of ANITA in compliance with this section of the Policy and, in general, with the applicable legal framework.

4.1 Access

Being automatic the individual recognition of persons accessing the system, logical security mainly concerns the phase of authentication. A set of guidelines is given below; on the other hand, technical implementation details are beyond the scope of this Policy.

1) The systems must be checked for the compliance with access policies and standards (in accordance with the Policy of every LEA) and detect unauthorized activities.
2) Access monitoring makes it possible to verify the effectiveness of the control objectives and their implementation. Event recording procedures allow:
    1. The recording of all activities with negative results (anyway, each LEA may consider broadening the scope of logging activities);
    2. The history of all unauthorized access attempts;
    3. The sequence of system alarms and malfunctions;
    4. The date and time of log on and log off.
3) The result of monitoring activities has to be periodically reviewed.
4) Log files must be adequately protected against alteration and unauthorized access.
5) To guarantee inalterability, the logs have to be sent to a special server, not accessible to the LEAs operators who works with ANITA.
6) The logs are kept on file for up to two years and are reviewed annually or in case of anomalies / reports.
7) The activities of system administrators of ANITA in the LEAs departments and operators are recorded chronologically.
8) The password is never readable, not even when typed in by the user. Passwords are stored in an encrypted form, being in a manner that prevents even them from being identified by who is responsible for their management. Accordingly, no one has a way to find a user password if it has been forgotten. In this case, the only option is to delete it and generate a new one.
9) When a new user ID is activated, an initial password that will expire upon the first login has to be generated, obliging users to input a new personal password known only by them.
10) These credentials allow the authentication and therefore the access to the systems relevant to the duties of the resource concerned.
11) Proper use of the credentials and, in particular, the password (the encrypted component) is fundamental for ensuring that only authorized personnel gain access to the system.
12) Nowadays there are many tools available on the market for discovering (cracking) passwords that can be easily downloaded from the Internet. Given current computer processing power, these tools can process high volumes of data in a very short time. For this reason, it is necessary to choose a complex password that complies with the security criteria established in this Policy.
13) Authentication is required for the access of all the LEAs. All the LEAs have to collaborate in order to comply with this Policy and further cooperate to set a common principle in the management of the access process to the tool which regards different situations:

a) the activation/deactivation of credentials that must be managed in the established manner, as part of a process in which an office communicates and authorizes the access/ leavers and the system administrator arranges for the related activation/deactivation, thus ensuring the appropriate segregation of functions;
b) authentication must be set up for each user and not for groups of users;
c) the right to access of a single user or of a specific group to which that user belongs to must be authorized by the internal rules of the LEA.

As explained in the description of the Knowledge Search (KS)[7], different users may obtain different results depending on the authorizations obtained on their profile (Figure 1) and on the settings of the portal (Figure 2), so it is necessary to balance these "personalized" research methods with the need of cooperation mentioned in the previous paragraph.

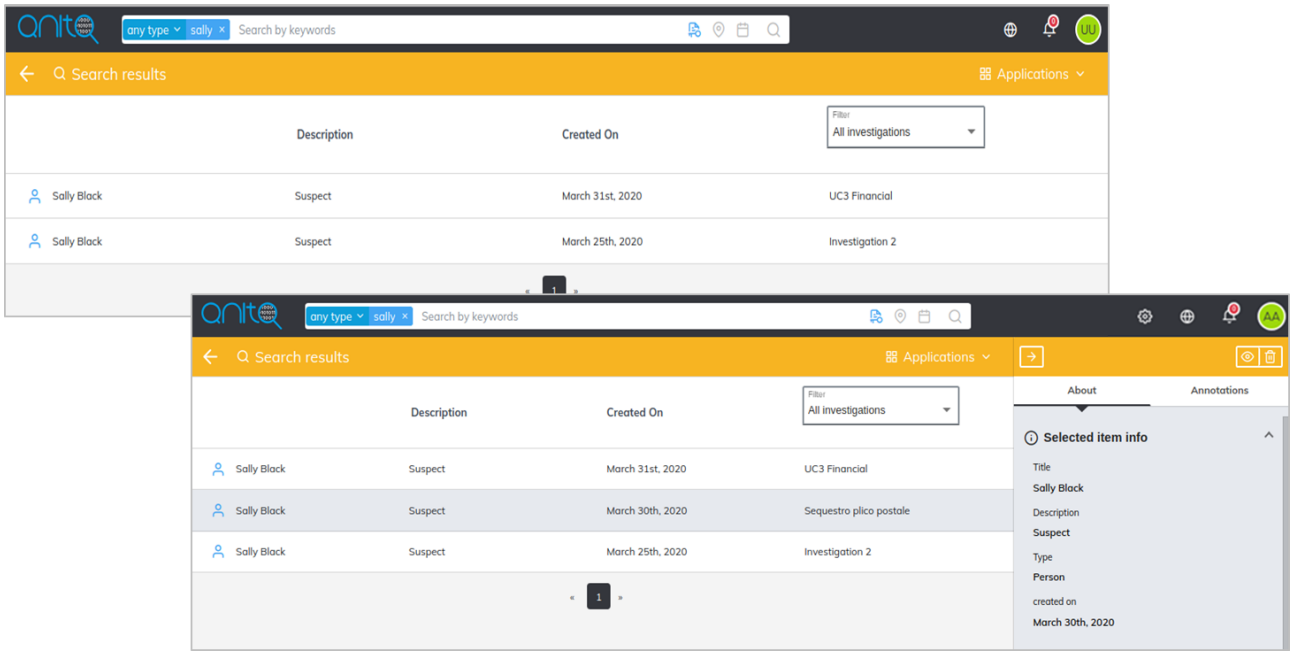


Figure 1: Knowledge Search results

[7] See for more details the paragraph 2.2.2. Knowledge Search in D9.6 – ANITA System – Update, page 24.

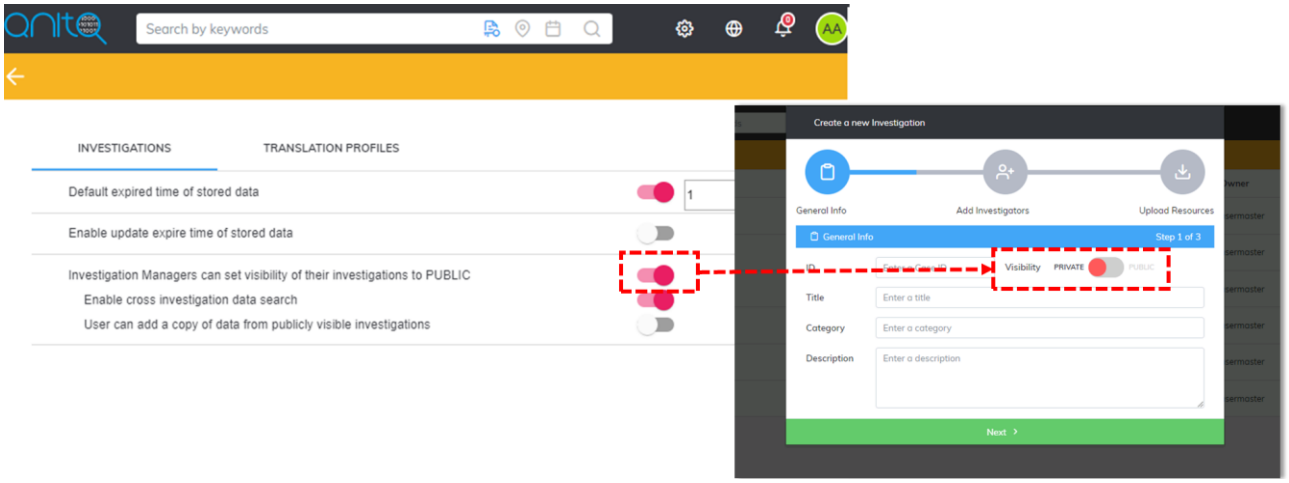


Figure 2: Public / Private configuration by the Investigation Manager

With the purpose of guarantee a secure and transparent cooperation between the LEAs the tool has been designed with "ad hoc" features which permit to: the "enable the cross investigation data search", using the related function (Figure 3) and it has been made available the opportunity to copy data from publicly visible investigations (Figure 4).

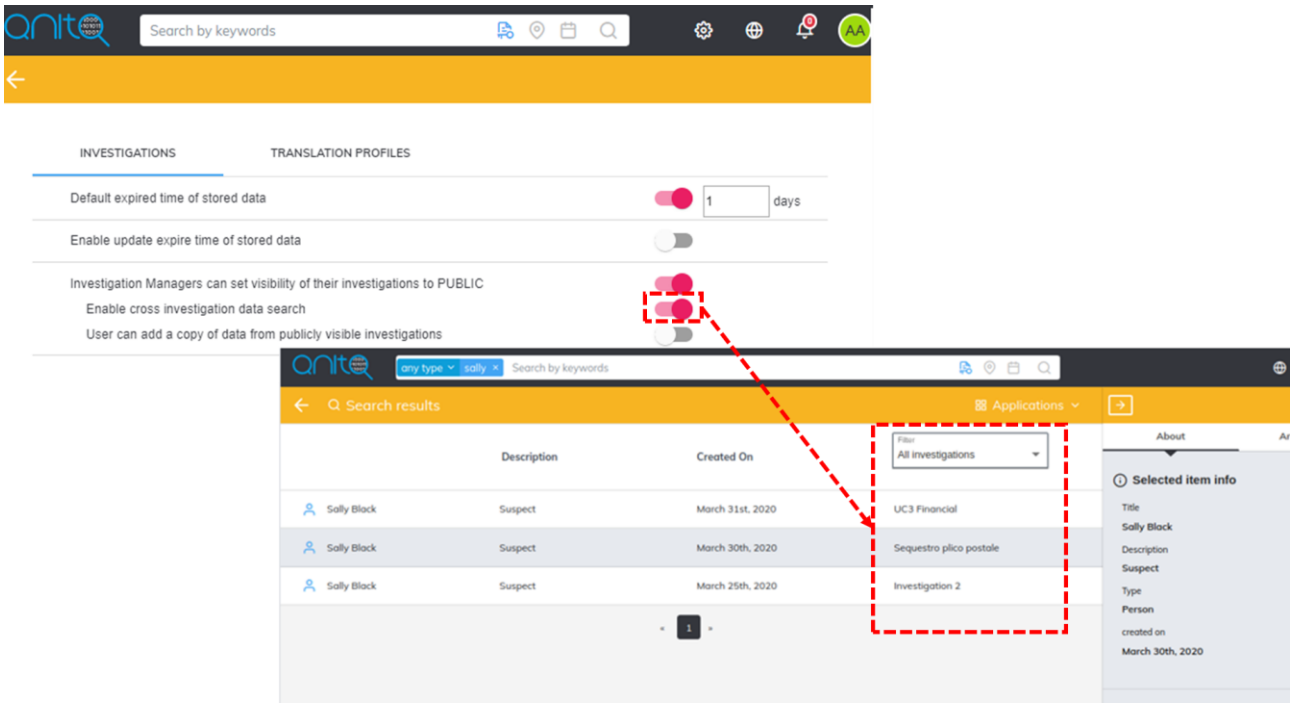


Figure 3: "Enable cross investigation data search" function

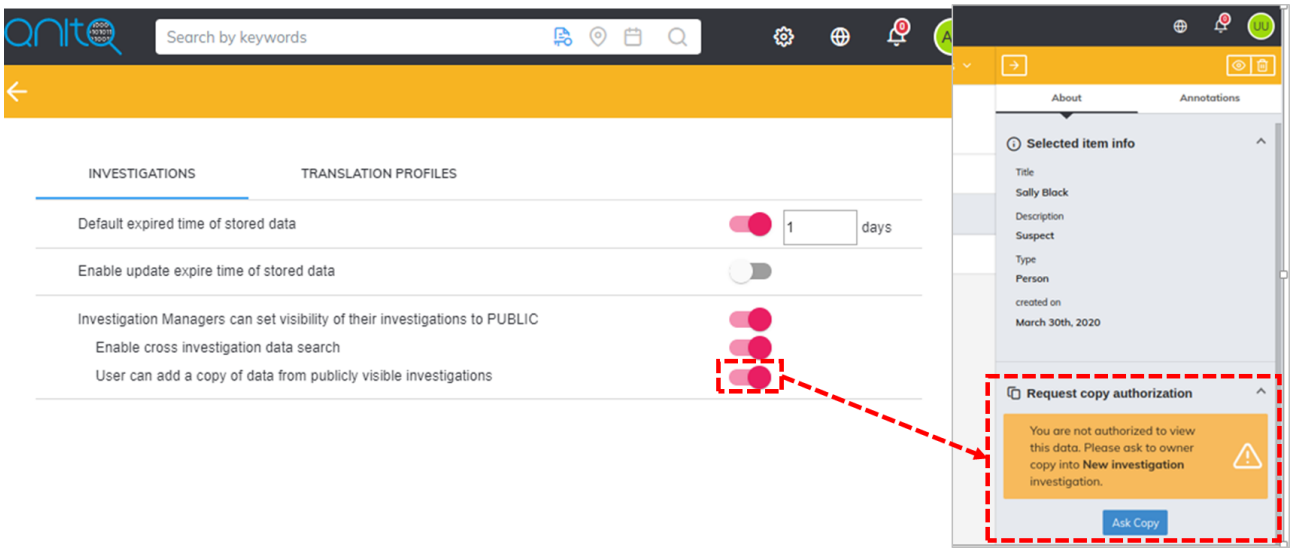
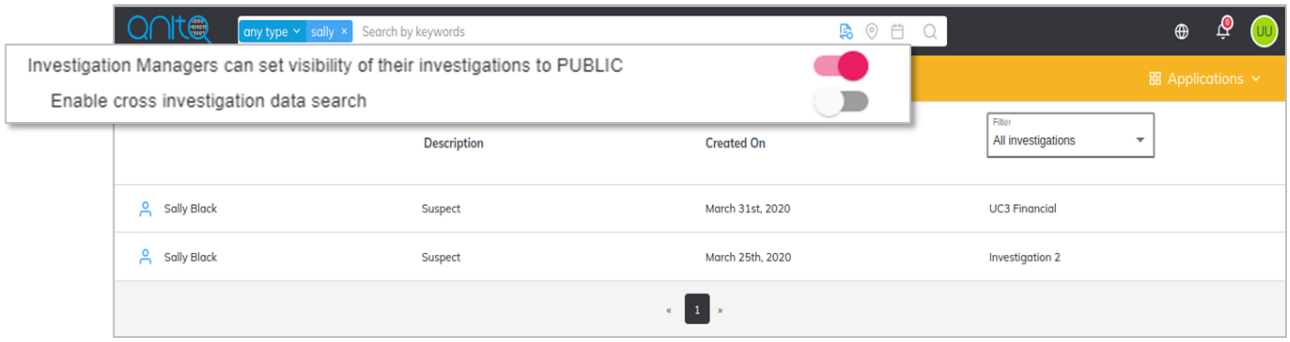
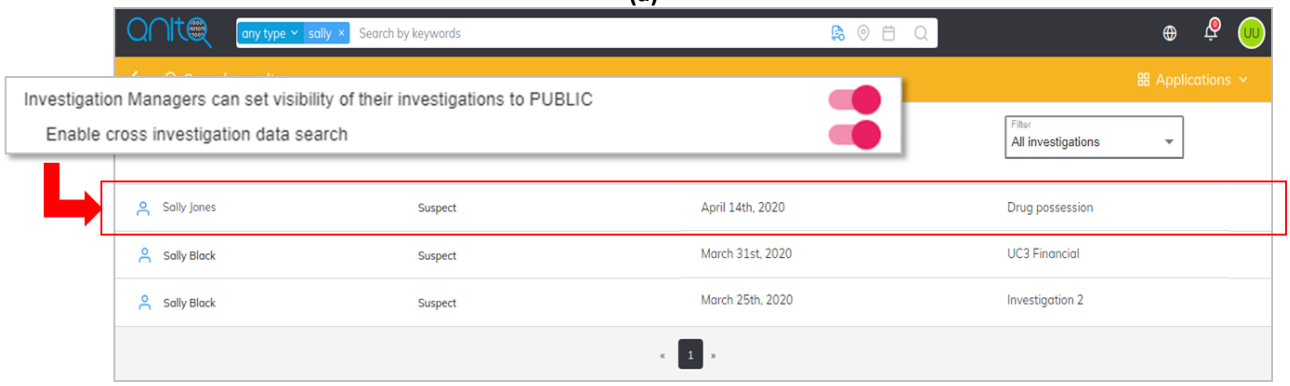


Figure 4: "Copy data from publicly visible investigation" function

In a case as the one displayed in Figure 3, if the function is turned on, the results produced may derive both from the public investigations (open to all the users) and the information related to the investigation to which the investigator was assigned to (Figure 5).



(a)



(b)

Figure 5: Difference between (a) the "only assigned" investigation results and (b) the cross-investigation function activated

Once the results obtained from public investigation and more in specific from another ongoing investigation, the opportunity to ask for a copy of those results has been created through a specific authorization instrument.

In fact, investigations having to respect different confidentiality levels and the approval from specific bodies are handled with a process able to ensure the protection of the information until a specific request is brought to the attention of the Investigation Manager. As illustrated in figure 4, if the function "user can add a copy from publicly visible investigations" is turned on, the user may access to the information related to the other investigation through the "request copy authorization" message, which permits to access to the information pertaining to a different investigation. The request will contain the reason of the need (Figure 6 and 7) of the information and will be presented to the other Investigation Manager.

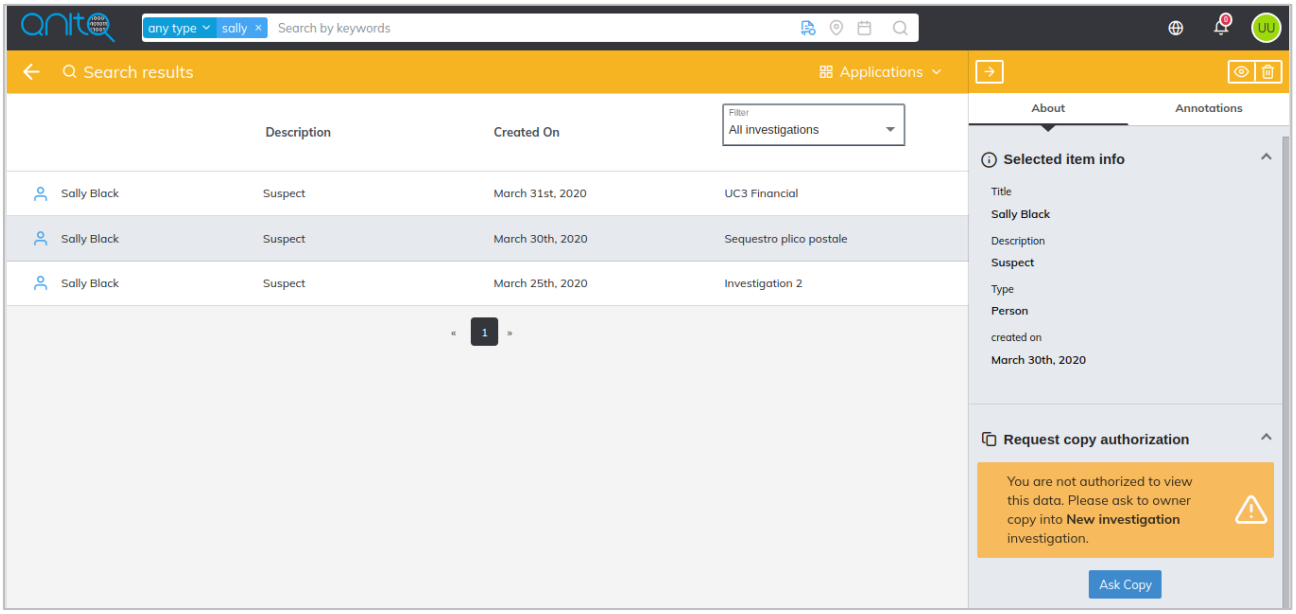


Figure 6: The "request copy authorization" function

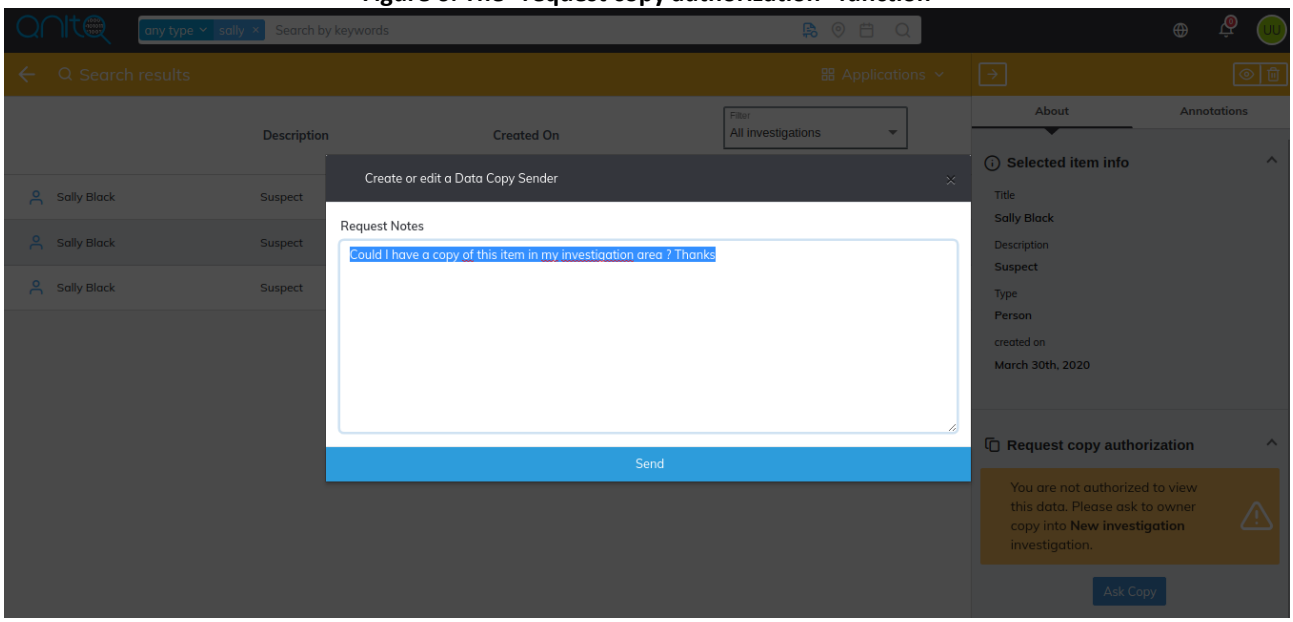


Figure 7: The "Request Notes" window to ask for information related to a different investigation

In case the information has been already required, the "pending" status is visible in the column of the "request copy authorization" (Figure 8).

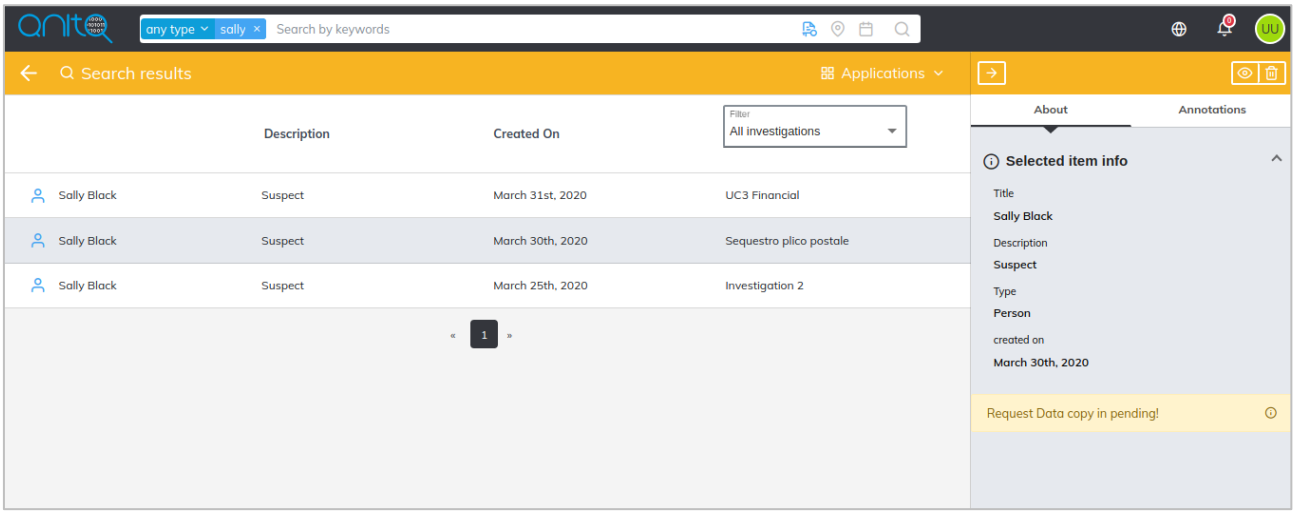


Figure 8: The pending status in the "request copy authorization" dashboard

At this point two situation may realize: the request can be approved (Figure 9) or denied (Figure 10); in this case – the denial of the request – the system will not permit to send other request for the same information[8].

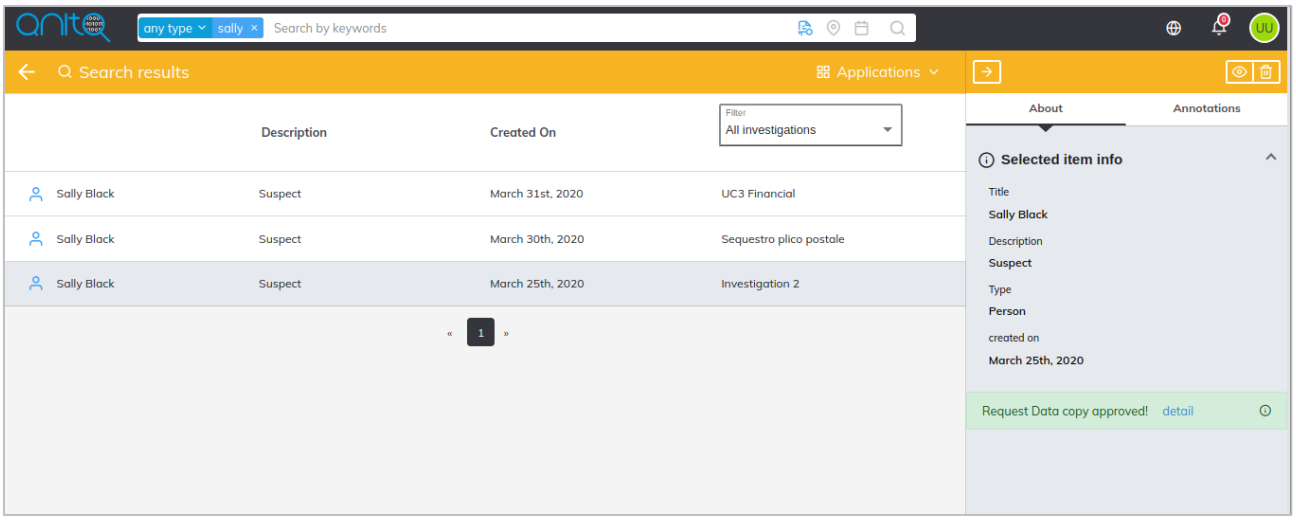


Figure 9: The approved request in the "request copy authorization" dashboard

[8] The hypothesis of data request denial is an extreme case in which mutual assistance may not be realized, as stated in article 25 of the Budapest Convention on Cybercrime (ETS 185 – Convention on Cybercrime, 23.XI.2001 - europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf).
However, the need and circumstances to obtain specific data may vary in different times, even if in a first stage the request was rejected. For this reason, the creation of a *rate limiting* mechanism to avoid the same request is under evaluation, to be adopted instead of the mechanism which excludes *in toto* the possibility to propose the same request.

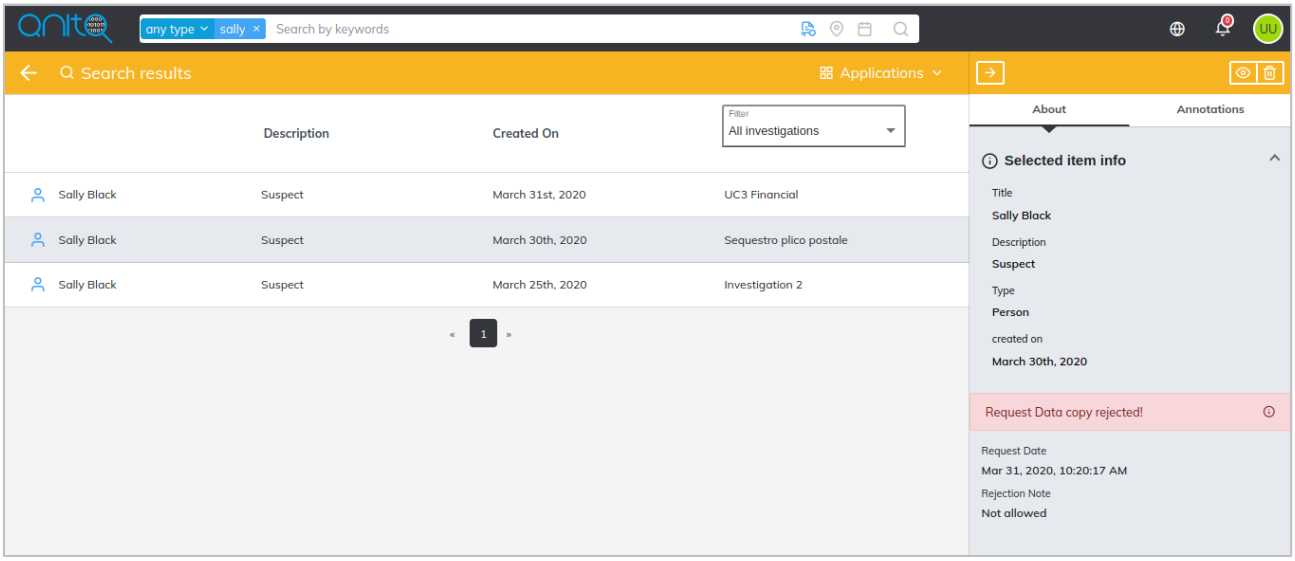


Figure 10: The rejected request in the "request copy authorization" dashboard

4.2 Information exchange in the network of the LEAs

As explained at the beginning of this section, one of the main goals of ANITA is to enable LEAs to break cybercrime down in darknets, especially through mutual collaboration in the use of the tool.

The tool will learn from the operators how to improve itself and then the operators will be able to collaborate in order to optimize the behaviours and searches of the tool, modifying indirectly the algorithm that is at the base of them, exploiting the power of machine learning to make the performance of the tool more efficient.

However, the algorithm may not be sufficient, so in order to overcome the technical limits imposed by the tool, the LEAs will have at their disposal technical and organizational/legal functionalities related to the exchange of investigative information and personal data to identify suspects and help in recognizing suspicious nicknames or particular markets in which conduct a specific inquiry on buying trends in the markets.

In this sense, LEAs operators may collaborate through the functions present in ANITA, indicating the type of information to be transmitted through the tool.

With regard to the different means through which LEAs may cooperate, Annex E of this Policy settles the transfer of personal data between LEAs.

Nevertheless, some rules must be established to make the cooperation process between LEAs more efficient and to protect the information assets exchanged. Regarding the exchange of information about actual investigations via the ANITA system, there are the following provisions.

1) The use of encryption to protect data assets will be useful to protect the collaboration between LEAs. The requirement to use or not use encryption will be based on the level of classification assigned to data gathered with ANITA that has to be shared with other LEAs.
2) Mobility is increasingly an essential element of competitiveness. However, while mobile devices give employees access to critical information and systems at any times, they also provide an entry point for data theft, malicious malware and other security threats to corporate systems. Mobile devices (smartphone and tablet or laptop) will be encrypted to reduce the risk to have unauthorized data processing and must not be used to share the data in the LEAs network.

3) For each internal or external connection involving the communication and/or transfer of ANITA data and information, adequate encryption has to be applied in transit.
4) All data assets using symmetric encryption algorithms shall only do so utilizing cryptographic keys of 128 bits or longer. Larger key spaces, however, are recommended for longer term security.
5) All data assets utilizing asymmetric encryption algorithms shall do so only exploiting cryptographic keys of 2048 bits or longer. However, larger key spaces are recommended for a long-term security.
6) Proprietary encryption algorithms are not to be utilized. Only those cryptographic algorithms that have undergone and passed public examination shall be considered acceptable for the use.
7) All the operators of the LEAs shall be properly trained and educated on the use and security of the encryption systems before they start the collaboration.

In particular, the tool has been designed to handle the data copy exchange in ANITA, giving the power to the Investigation Managers to accept or deny the requests from user of one investigation interested in information stored inside the framework of another investigation.

With this objective, a specific setting has been created at the portal administration level, as we saw before when the function "enable cross investigation data search" is turned on, it is possible to have visibility on information related to other investigations in addition to the one in which an investigator was authorized to work on.

This exchange may be realized excluding an automated exchange and adopting a supervised way, which permits to the owner of the investigation to assess the request and authorizes (or not authorizes) the copy data exchanges. ANITA has been created to handle the requests with the following actions:

1. A user *A-Investigator* sends a data copy request from the investigation *A* to the investigation *B* to get a copy of data *D* (that belong to Investigation *B*);
2. The owner of the Investigation *B* (namely *B-Manager*) is notified about the incoming request;
3. *B-Manager* can decide whether or not to approve the copy of data *D*;
    a. If the request is REJECTED, *B-Manager* can also include notes to explain the reason why the request was rejected;
    b. If the request is APPROVED, a physical copy of data *D* (namely data *D'*) is stored into investigation *A*, accessible by all users assigned to investigation *A*;
4. *A-Investigator* receives a notification when his/her request is closed (successfully or not).

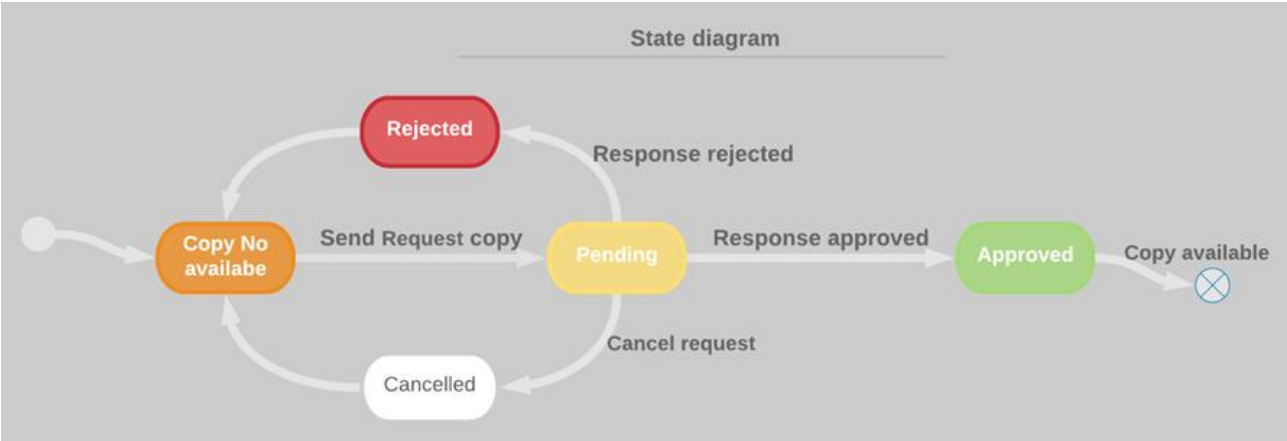


Figure 11: Diagram of statuses of a data copy request

The owner of the investigation has the visibility on the requests sent and their status, in order have an overview on data requests statuses (Figure 12).

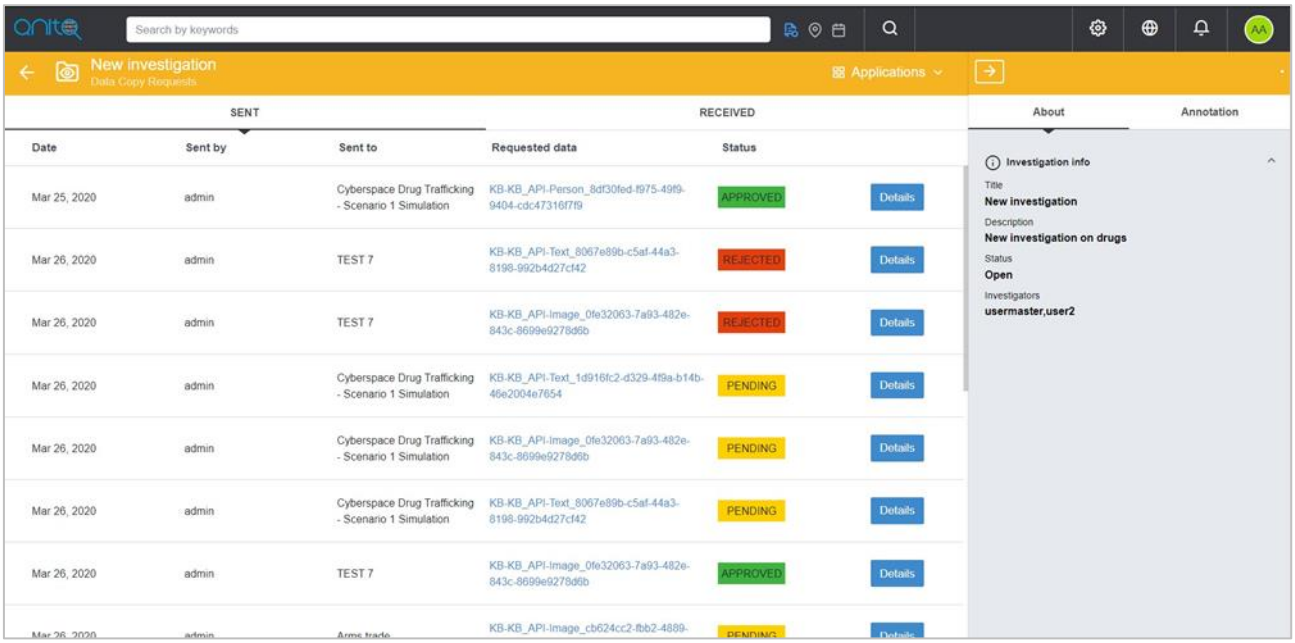


Figure 12: Data copy requests main page (owner of the investigation)

The owner will also have the opportunity to verify more in detail the status of the request (Figure 13) and reasons linked to the denial (Figure 14) or the information related to the investigation from which the request arrived in case of the approval (Figure 15).

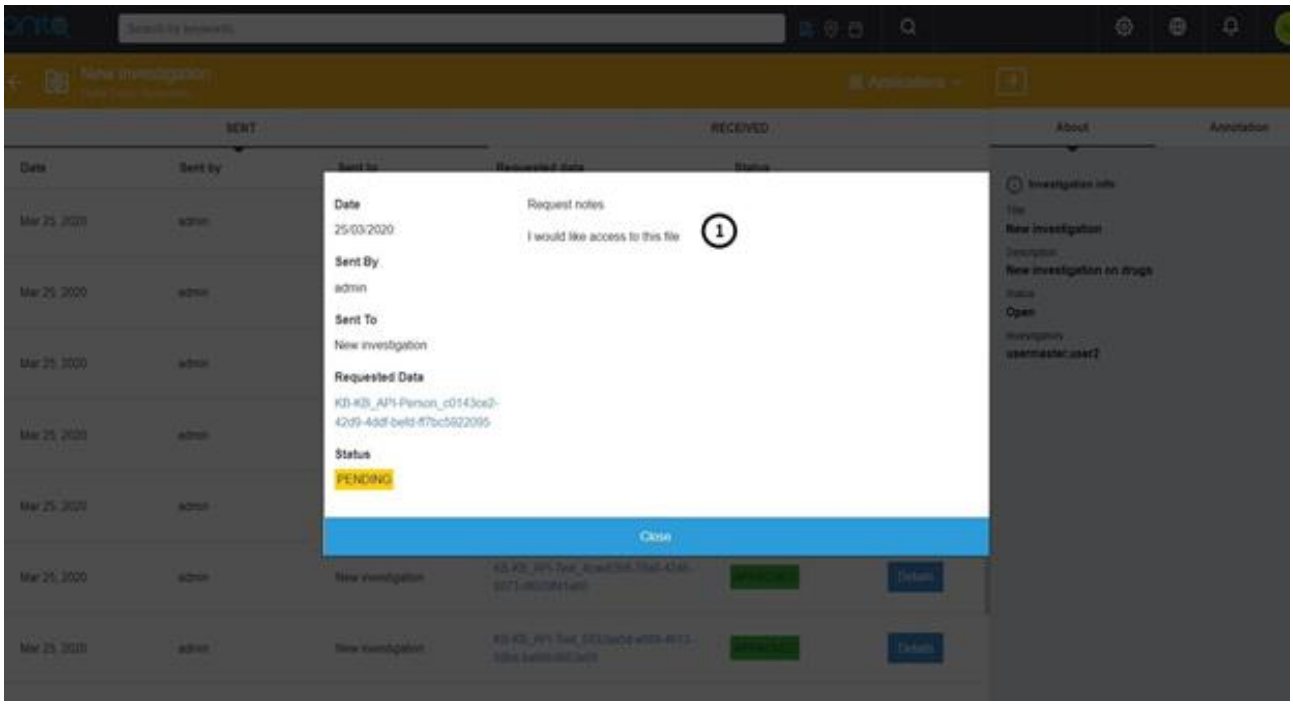


Figure 13: Detail box related to a data copy request (*pending* status)

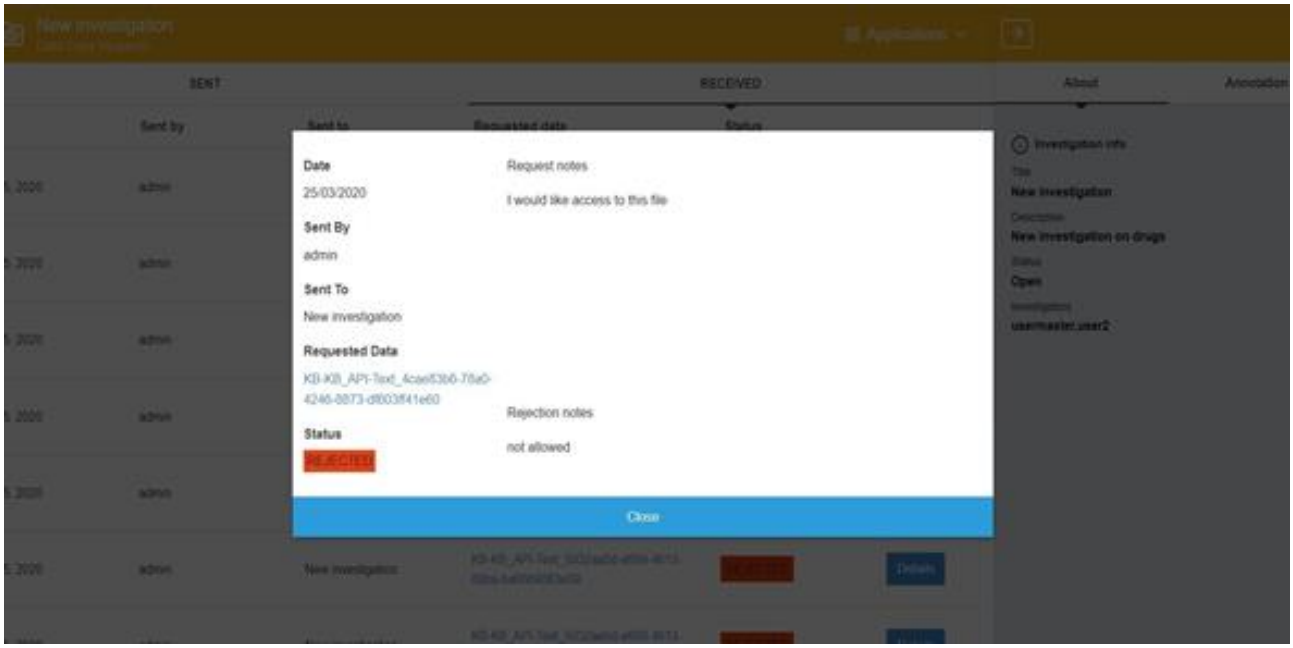


Figure 14: Detail dialog of a data copy request (*rejected* status)

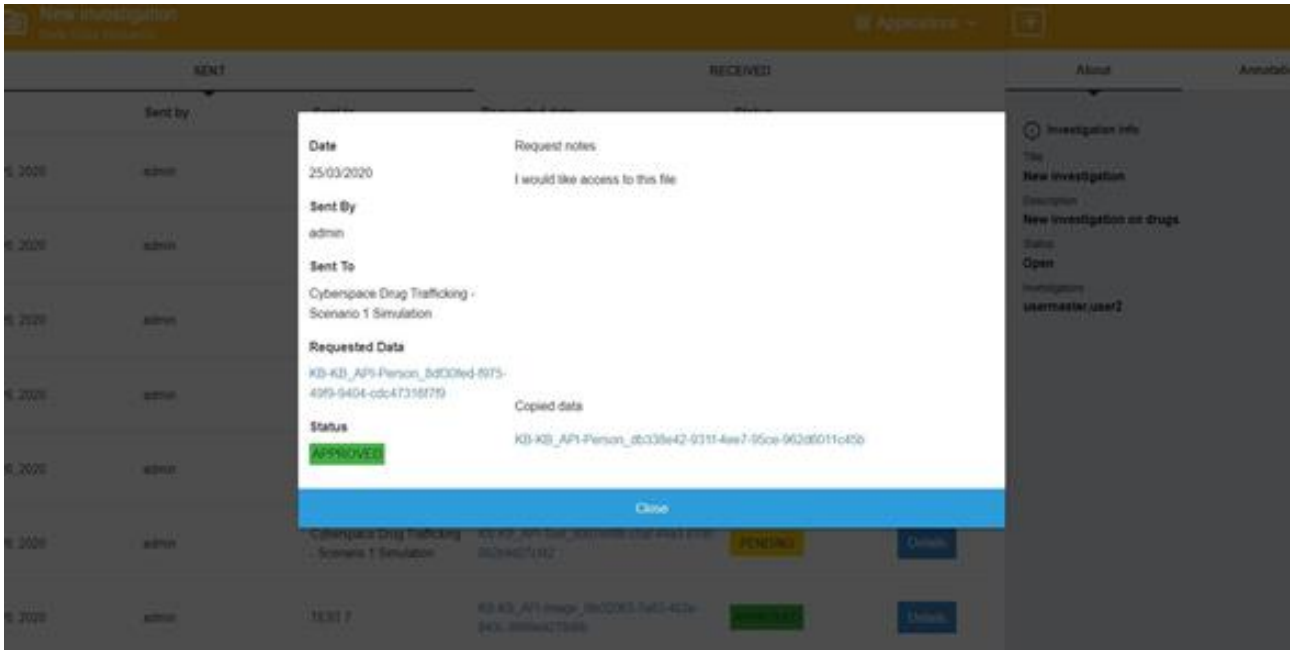


Figure 15: Detail dialog of a data copy request in (*approved* status)

From the other side, the subject who can handle the copy data request is only the investigation manager and from his/her side will have the following overview (Figure 16):

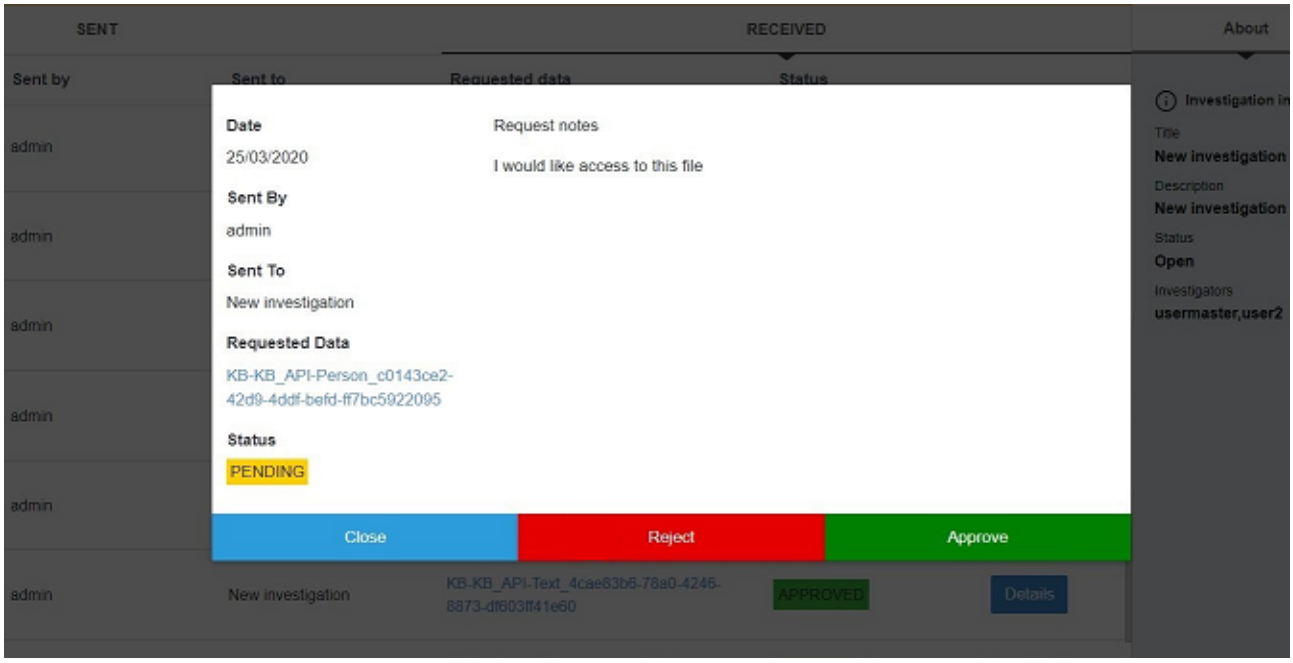


Figure 16: Detail dialog of a data copy request in *pending* status (investigator manager view)

Once the investigation manager will reject the request, a box appears to supply reasons behind the rejection (Figure 17). Meanwhile, if the request will be considered feasible, a box with the confirmation of the approval will appear (Figure 18).

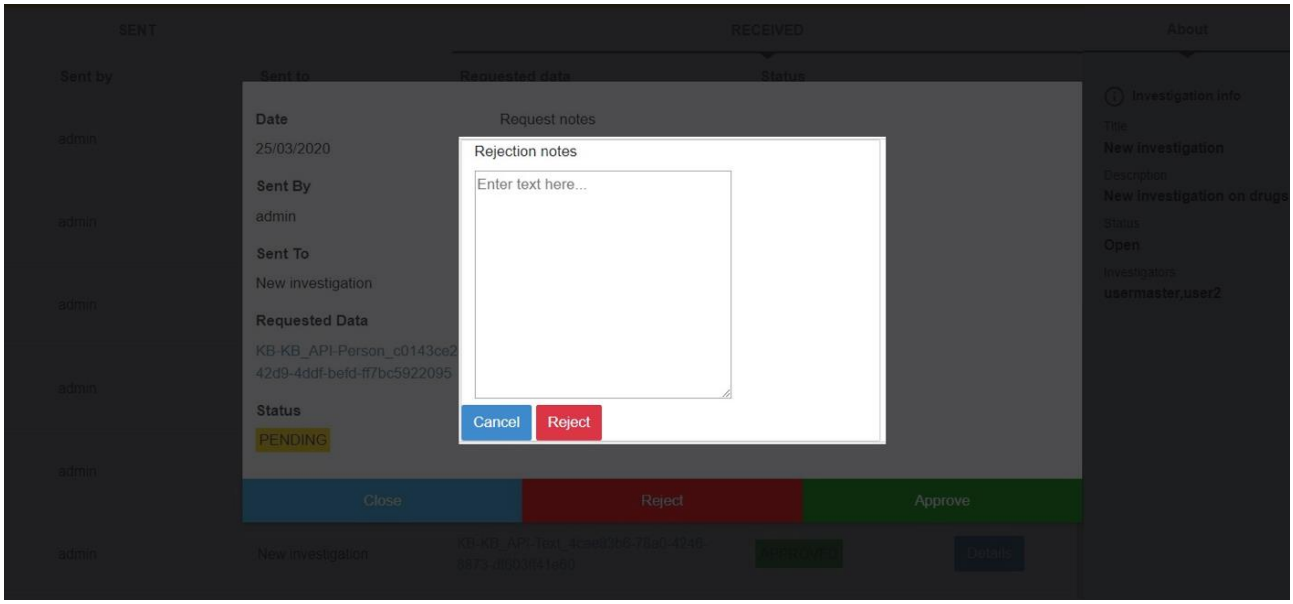


Figure 17: Dialog box to add notes to the rejection decision (investigator manager view)

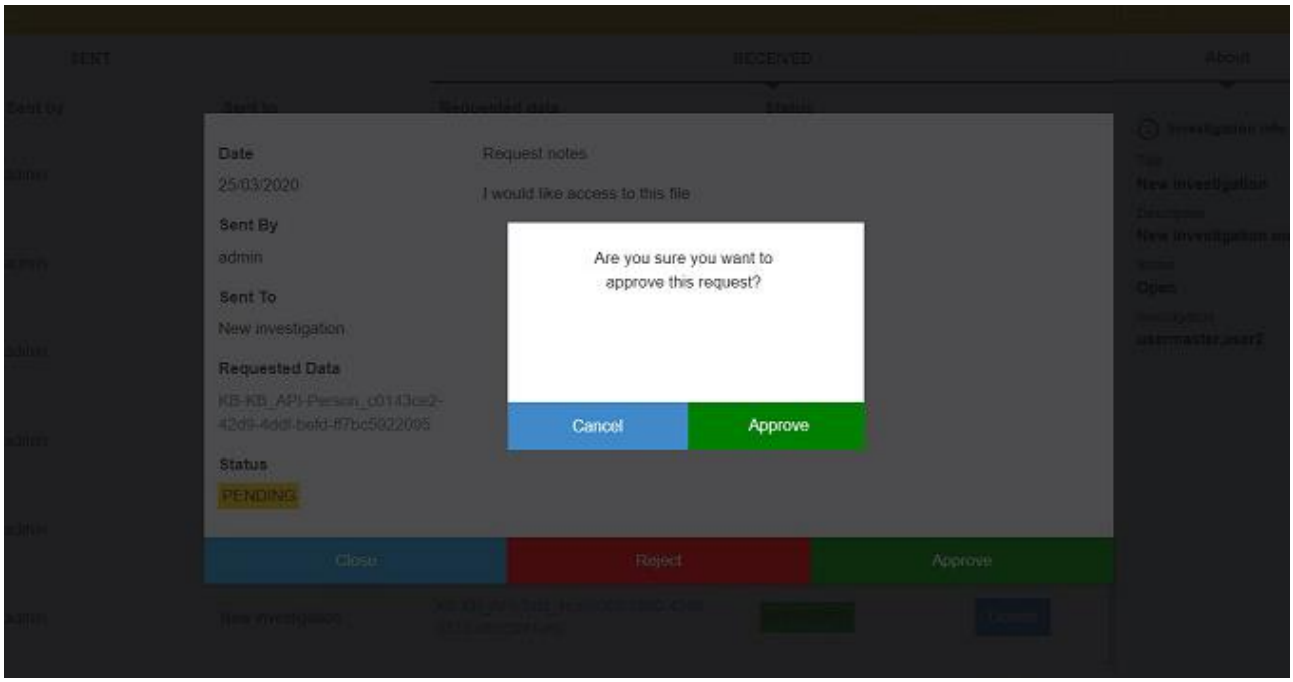


Figure 18: Dialog box appearing after the approval of the request (investigator manager view)

All those instruments will ensure the efficiency and the transparency as stated in article 5 of the GDPR, allowing to handle in a supervised way the data exchange concerning copies and requests emerging from the investigations using ANITA.

4.3 Cooperation with Authorities of third Countries

Online illegal trafficking often has links beyond the territory of the European Union. In this regard, in case of interest from international organisations - such as the International Criminal Police Organisation "**Interpol**" - on ANITA, the rules of this paragraph shall apply. Therefore, LEAs should be able to exchange personal data with authorities of third Countries to the extent necessary for the accomplishment of their tasks.

All Member States are affiliated to Interpol, which fulfils its mission by receiving, storing and circulating data in order to assist competent Law Enforcement Authorities in the prevention (of) and fight against international crimes. Therefore, it is appropriate to strengthen cooperation between LEAs and Interpol by promoting an efficient exchange of personal data whilst ensuring the respect for fundamental rights and freedoms regarding the processing of personal data using ANITA. When personal data are transferred from LEAs to Interpol, the provisions of Europol Regulation and GDPR, in particular those on international transfers, shall apply.

In order to be compliant with the purpose limitation principle, it is important to ensure that personal data will be transferred by LEAs to Union bodies, third Countries and international organisations only if necessary, for preventing and combating crimes that fall within the objectives of ANITA. To this end, it is necessary to ensure that, when personal data are transferred, the recipient gives an undertaking that the data will be used by the recipient or transferred onward to a competent authority of a third Country solely for the purpose(s) for which they were originally transferred. In any event, the transfer of data should take place in compliance with Europol Regulation and GDPR.

Using ANITA, LEAs shall be able to transfer personal data to an authority of a third Country or an international organisation on the basis of a decision of the Commission, finding that the Country or international organisation in question ensures an adequate level of data protection ('adequacy decision'), or, in the absence of an adequacy decision, an international agreement concluded by the Union pursuant to Article 218 TFEU, or a cooperation agreement allowing for the exchange of personal data concluded between the LEA and the third Country.

As general rule that governs the whole project, any information which has clearly been obtained in evident violation of human rights shall not be processed by ANITA.

5 Annex

A) Event Sheet

EVENT SHEET	
CODE	
Date on which the abnormal event occurred, and/or date on which the Personal Data Breach is presumed to have occurred (specifying that this is merely a presumption)	
Date and time on which the Data Controller / Data Processor became aware of the Personal Data Breach	
Source which reported the Personal Data Breach	
Type of Personal Data Breach	
Categories of Personal Data affected	
Description of the abnormal event	
Number of affected Data Subjects	
Number of Personal Data records which are presumed to have been breached	
Place where the Data Breach occurred	
Brief description of the Personal Data processing and/or storage systems	

involved, as well as their location	

B) Personal data breach sheet

PERSONAL DATA BREACH SHEET		
EVENT CODE[9]	CLASSIFICATION[10]	RISK[11]

[9] Enter Event Sheet Code.

[10] The DBAMU will classify an analysed event according to the following categories:

- *Unlawful destruction of Personal Data;*
- *Unlawful loss of Personal Data;*
- *Unlawful modification of Personal Data;*
- *Accidental destruction of Personal Data;*
- *Accidental loss of Personal Data;*
- *Accidental modification of Personal Data;*
- *Unauthorised disclosure of Personal Data;*
- *Unlawful access to Personal Data.*

[11] The Personal Data Breach must then be assessed according to the following risk levels:

- ***NONE***
- ***LOW***
- ***MEDIUM***
- ***HIGH***

These risk levels refer to the probability that one of the following adverse effects may occur, to the detriment of natural persons (even if those persons are not affected Data Subjects), as a result of the Personal Data Breach:

1. Discrimination;
2. Identity theft or fraud;
3. Financial loss;
4. Damage to reputation;
5. Loss of confidentiality of Personal Data protected by professional secrecy;
6. Unauthorised reversal of Pseudonymisation;
7. Significant economic or social disadvantage;
8. Deprivation or limitation of rights and/or freedoms;
9. Loss of control over Personal Data;
10. Other physical, material or non-material damage to natural persons.

C) Register of personal data breach

Event				Consequences	Measures taken	Notification to the Data Protection Authority		Communication to Data Subjects	
Code[12]	Irrelevant	False Positive	Relevant			Y/N	Date	Y/N	Date

D) Template for Communication of a Personal Data Breach to Affected Data Subjects

Under Art. 34 of the General Data Protection Regulation (EU) 679/2016, _____, as Data Controller, hereby informs you of the occurrence of a personal data breach, which took place on _____[13], at _____[14], and which _____ became aware of on _____[15].

A) Description of the nature of the Personal Data Breach:

a) Where did the Personal Data Breach occur?

b) Type of personal data breach, e.g.:

- Unlawful access to Personal Data (*where the affected Personal Data was not unlawfully copied by the persons accessing the data*);
- Unlawful copying of Personal Data (*where, in spite of the Personal Data Breach, the affected Personal Data are still available in the Data Controller's systems*);
- Unlawful modification of Personal Data (*where, in spite of the Personal Data Breach, the*

[12] Enter Event Sheet code.

[13] Either enter a specific date, a presumed date, or a timeframe during which the breach may have occurred (e.g. between X and Y).

[14] Either enter a specific time, or mention that the exact time cannot be determined.

[15] Specific time and date.

affected Personal Data are still available in the Data Controller's systems, but have been unlawfully changed);

- Unlawful or accidental loss of Personal Data (*where the affected Personal Data are no longer available in the Data Controller's systems and the identities of the persons behind the Personal Data Breach are unknown*);
- Theft of Personal Data (*where the personal data are no longer available in the Data Controller's systems and instead are known to be the possession of the author of the breach or another third party*);
- _____

c) Devices breached, e.g.:

- Computer;
- Corporate Network;
- Mobile device;
- Backup tool;
- Paper documents;
- _____

d) Categories of Personal Data affected by the Personal Data Breach, e.g.:

- Personal identifying data (name, surname, telephone number, e-mail, address, etc.);
- User access and authentication data (username, password, customer ID, other);
- Personal data revealing racial and ethnic origin;
- Personal data revealing religious beliefs;
- Personal data suitable to reveal philosophical beliefs;
- Personal data revealing political opinions;
- Personal data revealing political party membership;
- Personal data revealing trade union membership;
- Personal data revealing membership of religious associations or organisations;
- Personal data revealing affiliation with philosophical associations or organisations;
- Personal data concerning health;
- Personal data concerning a natural person's sex life;
- Judicial Data;
- Genetic Data;
- Biometric Data;
- Copies of physical documents taken by images generated electronically;
- Still unknown;
- _____

This breach is likely to present a high risk to your rights and freedoms.

B) Describe the likely consequences of the Personal Data Breach;

C) Describe the technical and organisational measures taken to address the Personal Data Breach and, if necessary, to contain the Personal Data Breach or to mitigate its possible adverse effects;

If you wish to obtain more information about this breach, please contact the DPO.

Contact details:

a) Name and surname of the DPO
b) E-mail address;
c) Certified electronic e-mail address;
d) Physical address;
e) Dedicated telephone number;
f) Dedicated fax number;

Date, Place _____

_____ ***[The DPO]***

Kind Regards

E) Data Sharing Agreement

This Data Sharing Agreement (hereinafter, "Agreement") is made and entered into force the ___ (the "Effective Date") by and between [Entity2] ("End-users that own the data sets") and ("Technical Partner"). [entity1] and [Entity2] may be individually referred to in this Agreement as a "Party" and collectively as the "Parties."

PRELIMINARY STATEMENTS

1. [entity1] [LEA's activity description]
2. [entity2] intends to conduct the research (the "Research") described in the protocol (the "Research Protocol") that is attached to this Agreement as Attachment A – [title of the attachment] and

desires access to [entity1] Data and other Confidential Information (defined below) for the sole purpose of conducting the Research.

3. [Entity2] is willing to share its Confidential Information and/or Data in a pseudonymized form with [Entity2] for use in conducting the Research in accordance with the terms of this Agreement.
4. [entity2] shall comply with all applicable laws, including those affecting personal data and ethical reviews of the Research, in connection with the performance of the Research and its obligations under this Agreement, including but not limited to, obtaining and maintaining all licenses, permits, authorizations, consents and waivers from relevant regulatory authorities and/or independent ethics committee(s) required to conduct the Research. [entity2] acknowledges that, to the extent it processes any personal data (as defined under applicable data protection laws) contained in [Confidential Information and/or Data pursuant to this Agreement, it shall do so as a data controller or its equivalent under such laws and shall process such data only in accordance with such laws.
5. [entity2] shall not attempt to identify the data subjects from whom the [entity1] Data was generated and shall not combine the [entity1] Data with data from other sources that could lead to identification of any individual.
6. [entity2] has the authority to and shall bind and ensure compliance by all Research Personnel to the terms of this Agreement.
7. The Confidential Information and/or Data is not intended to and shall not be used for commercial purposes, including for the benefit of any commercial third party; this restriction shall not apply to the subsequent use of any published Research Results by third parties.

The Parties agree as follows:

1. Definitions

“Confidential information” or “Data” means disclosing [entity1] confidential and non-public information provided by [entity1] to [entity2] under this Agreement. This Confidential Information and/or Data includes: [short description of the type of data, subject matter of data]. This Confidential Information and/or Data is described in the detailed technical identification of the Data which is attached to the Agreement as Attachment 2; this is also the form in which [entity2] will receive the Data.

“European Data Protection Law” means all laws and regulations applicable, following the relevant criteria on a case by case basis, for example, to the territory or Member State of the European Union where the Services are delivered and/or Data Subjects’ are resident and/or the Data Controller is established and/or however applicable on a case by case basis to the Processing of Personal Information.

“Publications” means any presentation, publication or other disclosure of the Research Results or otherwise, concerning, relating to or derived from the Research and/or [entity2]’s receipt, access and/or use hereunder of [entity1] Confidential Information and/or Data. Publications include, but are not limited to, manuscripts, abstracts and summaries of the Research Results.

“Research Personnel” means all persons conducting or assisting with the Research or otherwise having access to [entity1] Confidential Information and/or Data in connection with this Agreement, on behalf of [entity2].

“Research Tools” means any methodology, statistical methods, formulae or any other methods or tools used by [entity2] in conducting the Research, all of which must be specifically identified in the Research Protocol (Attachment A to this Agreement).

"Research Results" means the results generated by [entity2] through use of [entity1] Confidential Information and/or Data and otherwise in the course of performing the Research.
2. Intended use of the Confidential Information and/or Data and constraints

1. [entity1] agrees to provide [Entity2] with access to [entity1] Confidential Information and/or Data to conduct the Research. [Entity2] Confidential Information and/or Data shall be used solely and exclusively to (i) conduct the Research strictly in accordance with the Research Protocol and (ii) ... and (iii) ... The Research Protocol may be amended only upon formal written amendment to this Agreement duly executed by both parties. For avoidance of any doubt, [entity2] has no rights to transfer [entity1] Confidential Information and/or Data to any third party outside the Consortium.
2. Purpose of Information Sharing. The Parties are entering into this agreement, and [entity1] is granting [Entity2] access to the Information (defined in section 1), for the purpose of [TBD]
3. Disclaimer of Warranties by [Entity1] CONFIDENTIAL INFORMATION AND/OR DATA IS PROVIDED "AS IS" [Entity1] MAKES NO REPRESENTATIONS AND EXTEND NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO ANY [entity1] CONFIDENTIAL INFORMATION AND/OR DATA. [entity1] DISCLAIMS ALL WARRANTIES OF NON-INFRINGEMENT WITH RESPECT TO ANY THIRD-PARTY RIGHTS AND TITLE, INCLUDING PATENT RIGHTS AND USE THEREOF.
4. Intended use of the information: how the receiver will use the information; what studies will be performed, and for which expected outcomes.
5. Restrictions list on how the information or data findings can be used (e.g. need for [entity2] to document how the information are used; possibility to share, publish or disseminate data findings and reports without the approval or review of the provider).

3. Methods of data sharing

1. Identify the way in which data will be transferred from the [entity1] to [entity2] (physically or electronically?)
2. If data are to be sent over the Internet, how can a secure connection be guaranteed?
3. Will the data be encrypted, pseudonymized or anonymized before being transferred?

4. Rights to use research tools and research Results

1. Ownership of the research results based on the data will belong to the [entity2].
2. Establish the possibility for [entity2] to use the data to explore additional research questions without the approval or consent of the [entity1].
3. [entity1] agrees to grant [entity2] a) the access and the right to use all Research Tools for the purpose of reproducing the Research and b) the right to use and disclose Research Results for any lawful purpose whatsoever. [entity2] shall provide reasonable assistance to [entity1] in interpreting the Research Results.

5. Term and Termination
This Agreement will expire on the completion of the Research and completion of the publications included in the Publication Plan but in no event later than three (3) years from the Effective Date. [entity1] may terminate this Agreement for [entity2] material breach of its terms, where the breach is not cured within thirty (30) days following receipt of written notice of same. Upon termination or expiration of this Agreement the rights and obligations of the Parties which have accrued hereunder shall survive in accordance with their terms, and [entity2] right to use [entity1] Confidential Information and/or Data shall immediately cease. The terms of Sections 5 (Term and Termination), 6 (Safeguards around data), 7 (Confidentiality), 8 (Publications), 9 (Miscellaneous) shall survive the expiration or termination of this Agreement.

6. Safeguards around Data
   [entity2] shall use appropriate safeguards to protect the Data from misuse and unauthorized access or disclosure, including maintaining adequate physical controls and password protections for any server or system on which the Data is stored, following Article 32 of GDPR and taking any other measures reasonably necessary to prevent any use or disclosure of the Data other than as allowed under this agreement.
   1. Definition of minimum-security measures
   2. Definition of the level of access to data (each personnel of [entity2] has the same level or will some people have restricted access?)
   3. Erasure/restitution of shared data [storage limitation] and erasure of any copy of the shared data after the termination of the Agreement

7. Confidentiality

1. [entity1] information must be marked as confidential.
2. For avoidance of any doubt, [entity1] Confidential Information includes, but is not limited to,

   [entity1] Data as defined in Paragraph 1.

3. Confidential Information and/or Data does not include information to the extent that: (i) it is or becomes in the public domain through no breach of this Agreement; (ii) the [entity2] lawfully can demonstrate it received from any third party without restriction as to use or confidentiality or was known to the [entity2] prior to the time of disclosure by the [entity1]; or (iii) it is independently developed by or for the [entity2] by persons without access to the Confidential Information and/or Data.
4. Upon the termination or expiration of this Agreement, [entity2] will promptly return or destroy, at [entity1]'s request, all Confidential Information and/or Data in [entity2] possession or control, together with all copies, summaries and analyses. However, [entity2] is entitled to retain one copy of Confidential Information and/or Data for the sole purpose of determining its obligations under law or this Agreement.

8. Publications

1. [_] shall provide [_] with copies of any proposed publication or presentation at least [days/week/months] in advance of the submission of the proposed publication or presentation to a journal, editor, or other third party.
2. [entity1] will have [... days/weeks/moths] after receipt of the materials to object to the proposed presentation or publication, because there is patentable or potentially patentable subject matter that needs protection.
3. If [entity1] does makes an objection, [entity2] shall refrain from publishing or presenting the materials.
4. If [entity1] does not respond to [entity2]'s submission of materials for its review, [entity2] may proceed to publish or present these materials.
5. Decide if [entity2] can publish or present any material relating to the Research at the end of the Project

9. Miscellaneous

1. Entire Agreement. This Agreement and any attachments hereto set out the entire agreement of the Parties and supersede all prior agreements and understandings relating to its subject matter. This Agreement and any attachments hereto may not be altered, modified, or waived in whole or in part, except in writing signed by both Parties.
2. Governing Law. This Agreement and any claim, controversy or dispute related to this Agreement or the relationship of the Parties will be governed by the laws of the ...
3. Counterpart Signatures. This Agreement may be executed in counterparts or via electronic signature, each of which shall be deemed to be an original, and all of such counterparts or electronically signed documents shall together constitute one and the same Agreement.
4. List of Attachments.

   Attachment A – Research Protocol
   Attachment B: Detailed technical identification of the Data

In order to demonstrate their agreement, the Parties have executed this Agreement as of the Effective Date.

[entity1] [entity2]

By: _____ By: _____

Name: _____ Name: _____

Title: _____ Title: _____