VICTIM SUPPORT AND DATA PROTECTION

SOME CONCERNS AND PROPOSED SOLUTIONS FOR VICTIM SUPPORTERS

Victim Support Europe

CONTENT

INTRODUCTION

The introduction of new rules under EU GDPR – 2018

GDPR Glossary

APPLYING EU DATA PROTECTION RULES IN VICTIM SUPPORT SERVICES

Defining Personal Data

Legal Basis for Collecting Data

- Consent
- Contract as a legal basis for data processing
- Legal obligation
- Vital interest
- Legitimate Interest
- Public interest

Safely storing victims' data

Data processing by victim support organisations

Rights of Victims as Data Subjects

Data Retention

GDRP Compliant Referral to Specialised Services

Cross-Border referrals, including outside the EU

Special Categories of Data and criminal data

Victim information sheet

CONCLUSIONS AND RECOMMENDATIONS

INTRODUCTION

For decades now, society has relied on the help given to victims by organisations providing vital support services. Now more than ever, the core nature of victim services has been accentuated by the outbreak of COVID-19, with many countries declaring victim support an essential service – one that needs to be maintained even as the vast majority of social and economic activities are put on hold. Indeed, the European Commission, in its recent EU Victims Strategy, recognises the indispensable nature of victim support services.

At the heart of quality support services is the flexible response to the individual needs of victims - supporting the victim and their loved ones whilst doing no harm to either the victim, their loved ones or any third person. For this reason, victim support organisations follow strict ethical principles and aim to deliver an elevated standard of services to victims, with confidentiality as a founding principle in this provision of services to victims.

Arguably, long before the establishment of extensive data protection standards, victim support workers and organisations were at the forefront of protecting (victims') information. Indeed, ensuring confidentiality has been a fundamental standard for VSE, and its members, since its inception 30 years ago.

Victim support professionals have been ensuring their clients' privacy for many years. They have advocated for the interaction between counsellor and victim to be confidential and promoted this position in EU legislation on victims' rights. They have implemented data privacy in accordance with EU and domestic legislation, with great care and at a significant cost and investment.

Often, those supporting victims have had to balance the requirement to collect and store victims' data in a sensitive and prudent manner, while ensuring data-sharing in an ethical and efficient manner. This has been done using a variety of approaches. Some organisations only stored sensitive victims' data on a single paper copy, kept locked in a safe. Others opted for storing data on a single computer, which remained off-line. In certain situations, victim support organisations have gone as far as to avoid asking for, collecting, storing or processing any personal data from the victims they support.

Fundamentally – victim support organisations have been doing their best to build and maintain relationships of trust with victims and make sure the victims they serve feel safe.

Victim Support Europe has long recognised this important aspect of victim services. In our 2012 publication: Statement of Victims' Right to Standards of Service – we set out confidentiality standards that ensure members were committed to:

- **Holding in confidence information given to them by or about a victim - accordingly no member should disclose to any third party information received from or relating to a victim unless:**

[1] VSE has advocated for victim support services to be officially recognised as essential services. This has been recognised by the European Commission, which recommended this approach to all the Member States in the EU Strategy on victims' rights 2020-2025. See https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-258-F1-EN-MAIN-PART-1.PDF

[2] https://victimsupport.eu/activeapp/wp-content/files_mf/1348589602service_standard_rights.pdf

- the victim has consented, or
- there is a legal requirement to do so, or
- there is an overriding moral consideration

→ **having clear procedures for dealing with such situations**

→ **having a public complaints procedure for dealing with alleged breaches and any other complaints.**

We have continued to promote the necessity for protecting victims' data through our Standards and Accreditation system, which places the onus of ensuring victims' safety and confidentiality of victim support services on our (full) members.

THE INTRODUCTION OF NEW RULES UNDER EU GDPR – 2018

Whilst victim support approaches to data protection have been carried out within the framework of EU data protection rules that have been in place since 1995, the coming into force of the General Data Protection Regulation (the GDPR) in 2018, has had a significant impact on support organisations.

For many, the implementation of the GDPR has been close to overwhelming, with rules that should enhance victim safety sometimes putting at risk the very organisations that help the victims. The unintended risk of the GDPR is that data protection in victim support stops being driven by an inherent concern for victims' well-being and becomes a desperate attempt to conform with rules and avoid large scale fines.

To add to the complexity of an already sensitive situation, the rules are left deliberately vague. To be able to understand how GDPR should be applied requires significant external or in-house expertise at considerable cost.

Yet, when investment into GDPR compliance is made, organisations are still exposed to the different interpretations, by national data protection authorities, of the rules. This exposes even the most careful organisation to the risk of repercussions, indicating that the current system too often fails to respect the reality of victim support services.

What originated as legislation driven by (mis)behaviours of large profit-making businesses and the expansion of the internet is now applied horizontally and equally to everyone. This has created challenges for victim support organisations where issues – such as capacity, the importance of their mission or of their ability to cover financial penalties for any unintended mistakes – are not fully understood or considered.

Large international businesses can afford to build into their business model the risk of being fined for GDPR violations and can even take calculated risks to generate larger profits at the expense of potential data protection violations[3]. On the other hand, small organisations providing essential services cannot usually afford even the smallest mistake as even a minor fine could end their programmes and disrupt lifeline services to vulnerable victims.

Victim support services must balance data protection with multiple rights such as the right to privacy, the right to life and the right to justice – all three of which victim support organisations protect. This is not to say that the GDPR has not benefited the privacy of victims. Indeed, it has highlighted the necessity for all organisations, including support organisations, to have a clear legal framework, which ensures victims' data is properly protected.

[3] For example, in 2019 Google Inc was fined with € 50 million by CNIL – the French data protection authority, for breaches of GDPR – the highest GDPR breach fine to date. See more at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Every victim support provider needs to have clear and transparent policies on the collection, storage and sharing of victims' data.
These policies must ensure that:

data is stored safely and responsibly

access to sensitive victims' data is given to a limited number of specifically authorised personnel

those accessing data are trained to deal with data safely

those accessing data are held responsible for any potential breeches of victims' privacy

VSE has heard from support organisations, who are concerned that the GDPR framework has introduced rules that can be interpreted by 27 Member State national data authorities as they see fit. Support organisations have to rely on the various, often undisclosed, interpretations rather than working to one cohesive framework.

This lack of coherence can seriously undermine legal certainty. GDPR starts from the premise that all data controllers accept a certain level of risk in collecting and processing personal data. It is not up to the authorities to prove an organisation has failed to comply with GDPR, rather – due to the vague rules, and the understanding that it is impossible to fully protect personal data - organisations must prove they have NOT not-complied with GDPR!

Ultimately, there is concern that GDPR inhibits the ability of organisations to efficiently serve victims and that objectives of data protection could be achieved in a more proportionate, consistent, and co-ordinated manner.

Numerous discussions have taken place within VSE, and amongst our membership, on how to ensure compliance with strict, and sometimes quite demanding, formalities and to provide the best support to victims in need. In some organisations, this raised questions on and required changes in how victims' data is collected, stored, and shared.

This paper aims to help our members safely navigate GDPR, while ensuring victims' services. It also aims to initiate

a discussion at the European level on the operation of the GDPR from the perspective of civil society service providers, to explore problems arising from the implementation and interpretation of the GDPR, and to examine potential European and national solutions.

GDPR GLOSSARY

GDPR has introduced new terms in data collection. The interpretation of these terms as applied to the provision of victim support are given below:

data subject

Data subject – the individual, living physical person, whose data is subject to protection. Data subjects can be victims, their family members or, in cases of human resource issues, victim support workers.

data controllers

In the language of GDPR, victim support organisations are either **data controllers** or data processors (or both).

When an organisation decides the type of data to collect and for what purpose, it acts as a data controller. Usually, organisations will then process the data themselves, but they may entrust some or all that data to an external party for processing.

processing

Processing is any action using the personal data for an end purpose – to send victims' reminders for appointments, inform them of an upcoming trial, or have them participate in an information campaign. When processing is entrusted to an external organisation, victim support organisations must precisely describe and limit the reasons for sharing the data and must ensure that data is only used for that specific purpose. A contract outlining the specific purpose of the data processing should be created with the data processor.

If a victim is murdered, collecting personal data is not regulated by GDPR. However, identifying the victim could lead to the identification of their relatives or their neighbours, affecting their privacy. Therefore, identifying the dead can lead to the identification of living persons, whose data is subject to GDPR protection.

If a crime happens within a business environment, data related to legal entities can be freely collected, from the GDPR perspective. However, if that data can lead to identification of employees or owners of the business, GDPR is applied.

It is important to remember that GDPR is only applicable to digitalised data – hence, data stored in a digital form – an excel sheet, database, case-management system or other digital or electronic format – on a computer, USB stick, smartphone, or other digital storage. Asking a victim's name and other personal details, during the intake process, is not subject to GDPR if it is kept on paper and not stored in a digital format. The data might, however, be subject to other forms of limitation, depending on specific national legislation.

Therefore, if an organisation does not store victims' personal data digitally, in a way that could lead to their identity being known, GDPR is not applicable.

CASE STUDY

Organisation A has a paper-based filing system for victims' details, but keeps anonymised metadata for statistical purposes – number of victims, type of crimes, type of services provided, gender, language of victims etc. Organisation A is not a data controller or processor, from the perspective of GDPR, as the digital data is anonymous and the paper-based filing system for personal data is not subject to GDPR.

APPLYING EU DATA PROTECTION RULES IN VICTIM SUPPORT SERVICES

The main feature of GDPR protection focuses on the individual's right to control their own personal information and the legal basis for the obligations of the entity controlling and processing that data. Two fundamental questions need to be answered when determining if GDPR applies to an individual victim's support situation and whether the data can be processed.

Firstly, is the data considered 'personal', as defined by GDPR?

Secondly, does an organisation have a legal basis for controlling and processing such data?

DEFINING PERSONAL DATA

The GDPR defines personal data very broadly, as **any information relating to an identified or identifiable natural person.** To determine if information is personal:

- **The information must relate to an individual; and**
- **The individual can be identified from the information.**

According to Article 4(1) of the GDPR, personal identifiers include the name or other factors specific to the economic, cultural or social identity of a natural person. As such, there may be information about a person, which doesn't fall under GDPR if there is no identifying data such as name, date of birth, phone number or address to connect the information to the person.

The **collection of anonymised data for statistical purposes,** such as a victim's gender, age or type of crime, **will normally not be considered as data falling into the category of protected information** for the purposes of GDPR, as long as it is collected in such a way that the victim's identity remains unknown.

Yet, knowing whether GDPR is applicable or not is not always straightforward. A victim support organisation must always have a **legal basis to collect, store and process personal information** that could allow a victim to be identified.

CASE STUDY

A young man calls a victim support helpline seeking assistance. The support worker takes information on the crime and the needs of the victim. The victim states that he would like to arrange a meeting with a local victim support office.

The helpline worker takes the first name, email address and telephone number of the victim and inputs this into the organisation's case management system.

The information is then passed to the local victim support office (part of the same organisation) so they can contact the victim to arrange an appointment.

→ **Question: Does the GDRP apply in this situation?**

Answer: Yes – GDPR applies, since the victim is clearly identifiable from the data collected.

The helpline worker records some basic details of the crime (for example, that it concerned sexual abuse or online fraud) and needs of the victim; however, the worker did not record the caller's name, phone number or e-mail address. In the case management system, they note that the victim would like an appointment.

They give the victim the local branch's contact information and ask them to call or email for an appointment.

In the case management system, the case is assigned a reference number that will be passed to the local branch in the event the victim calls. The victim is provided with the same reference number for any subsequent calls.

→ **Question: Does the GDRP apply?**

Answer: No, GDPR does not apply, as it is not possible to infer their identity from the data collected.

The same facts apply as with Case 2. However, in addition to crime and needs information, the helpline worker also includes information that the victim is a Muslim, LGBTI victim of hate crime?

→ **Question:** does the GDRP apply?

Answer: It depends on whether it is possible to backtrack the victim's identity from the data collected. If it concerns a hate crime against a Muslim LGBTI victim that was covered by the media, it might indeed be possible to identify them even if no personal data is taken. If there is no way the caller's identity can be known, the GDPR would not apply[4].

LEGAL BASIS FOR COLLECTING DATA

GDPR aims at regulating the collection of personal data and provides several legal bases for data collection. **Consent, often seen as the main legal basis , is only one of several possible legal grounds for processing personal data under the GDPR.**

Consent can be complicated to obtain in the victim support context and may not be necessary. Exploring alternative legal bases

[4] However, when sensitive personal data is collected (such as religion, sexual orientation, gender identity), some other rules may also apply, so it might still affect the data collection process.

for processing data can improve the victim experience and help organisations maintain efficient processes.

The most appropriate legal basis will depend on the relationship of the data controller with the data subject. Responses from Victim Support organisations indicate that these depend on the national interpretation and approach of Data Protection Commissioners.

Article 6 GDPR provides for different bases for lawful processing. What are they?

Consent – the individual has given clear, unambiguous and fully informed consent for the controller to process their personal data for a specific purpose;

Contract – the processing is necessary for the performance of a contract an organisation has with the individual, or because they have asked the organisation to take specific steps prior to entering into the contract;

Legal obligation – the processing is necessary to comply with a legal obligation to which the organisation is subject;

Vital interests – for example, the processing is necessary to protect someone's life;

Performance of a task carried out in the **public interest** or in the exercise of official authority – the task or the authority must have clear basis in law;

Legitimate interests – the processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party unless there is a good reason, such as the protection of fundamental rights and freedoms, to protect the individual's personal data, which overrides those legitimate interests.

Any of the above examples is equally satisfactory, from the GDPR perspective - none takes precedence over the others; however, some forms are more practical and less burdensome for both victim and victim support organisation.

What is important to assert, however, is that:

- **There may be more than one legal basis to collect and process data, but one is enough;**
- **There is no hierarchy of legal basis – all are equally valid;**
- **There is no blanket authorisation to process data – each individual instance of data collection and processing needs to be justified on its own merit;**
- **Organisations need to be able to present, as requested, all data collected in relation to any data subject;**
- **Organisations need to be able to disclose any instance of data processing in relation to each data subject, whose data they collected;**
- **It is up to the organisations to ensure that their data collection and processing practices are not only GDPR compliant, but also ethical.**

Consent

Consent is often referred to as the 'default' legal basis for data collection and processing; but it may be one of the most complicated in the context of victim support. For consent to be acceptable under GDPR:

1. **Consent must be:**
   - Clear
   - Unambiguous
   - Fully informed
   - Recorded so that the victim support organisation can demonstrate that a victim has consented to processing of his or her personal data.
2. **The request for consent must be presented in a manner that is distinguishable from other matters to which consent may be given as well, and it must be gathered in a manner which will identify all purposes for which data is collected (if data is collected for case-management purposes, it cannot then be used for referral or for individual assessment).**
3. **If a victim does not want to share their personal data and they are told the provision of services is only possible if they it is given, consent cannot be considered to have been freely given. In such a situation, the legal basis for data processing should be found elsewhere – e.g. in legitimate interest.**
4. **A mechanism needs to be created by which a victim may easily withdraw his or her consent.**

In practice, to comply with these requirements fully and genuinely, the victim support worker will need to talk through a range of legal and formal issues before registering a victim's name or any other personal data.

The support worker needs to explain in detail to the victim the type of data to be collected, for what purpose the data is being collected as well as the procedure for withdrawing consent and have the victim sign a release form. If the support is being given on the phone, or if the victim has difficulty in signing the form (illiteracy, disability etc.), consent may be dictated for the caseworker to take down in writing alongside an explanation of the circumstances.

Weighed against the reality of providing victim support, as part of a **first response or first contact with the victim,** at a time when victims are likely to be highly traumatised and their cognitive abilities affected by the crime, it is obvious that this approach may be counterproductive. The procedure to acquire consent during a call to a helpline could make the phone call more complex and open to misunderstanding.

As the support organisation first contacted by a victim may not be able to give appropriate help and may refer the victim to a more appropriate provider, having to give GDPR information further complicates the situation.

CASE STUDY

A highly traumatised victim of sexual assault contacts a 116006 helpline to seek support. The assault took place very recently, but the victim has not yet reported the crime nor has she told anyone about the incident. The 116 helpline is run by Organisation A. The helpline worker asks the victim for her name during conversation, to be able to establish a personal connection, and writes it down on a piece of paper (**data collection point 1** – GDPR not applicable, because the name is only written on the paper), which will be destroyed as soon as the call is over. The helpline worker also collects other anonymous data (gender, age, date of the incident, gender and age of the alleged offender, previous victimisation etc.) and enters it into Organisation A's database for statistical and reporting purposes (**data collection point 2** – GDPR not applicable, because the data is anonymised).

The helpline worker tells the victim about the psychological support service that Organisation B is running and the victim decides she wants to talk to a psychologist. She gives her phone number to the helpline worker to have the psychologist call her back. The helpline worker sends the victim's name and phone number by e-mail to the psychologist with the message to call as soon as possible (**data collection point 3** – GDPR applicable, yes, because the name and phone number are written in an e-mail).

The psychologist calls the victim back after ten minutes. During the consultation with the psychologist, the victim reveals more details about her crime that the psychologist registers into Organisation B's case-management system. This includes the victim's name, phone number and some details about the circumstances of the crime (**data collection point 4** – GDPR applicable, because personal data is entered into the Org B's case-management system).

During the conversation with the psychologist, the victim also decides to have a rape kit collected by forensic specialists and to report the assault to the police. The psychologist sets up an urgent forensic appointment at the specialised centre, run by Organisation C. The specialised centre is in the same building as the psychologists' office, so he just walks there. He dictates the victim's name and contact details and some details regarding the circumstances of the crime to the receptionist who enters them into their internal case-management system (data collection point 5 – GDPR applicable, because personal data is entered into Org C's case-management system).

The Victim arrives at Organisation C for forensic examination two hours after her first call to the helpline.

At each point where GDPR is applicable, the legal basis for data processing needs to be determined and recorded appropriately.

> **"WHEN A VICTIM CALLS IN, THE LAST THING THEY WANT IS A COMPLICATED READING OF THEIR DATA PROTECTION RIGHTS. WE HAVE TO ALLOW THEM TO SPEAK AND WE NEED TO LISTEN IN A CARING MANNER. FINDING THE RIGHT WAY TO OBTAIN CONSENT TO RECORD INFORMATION IN THIS SITUATION IS REALLY TRICKY AND I'M WORRIED IT WILL PUT VICTIMS OFF"**
>
> – Victim Support Worker

Based on the above case-study, the victim's data is controlled and/or processed at least five times and on at least three occasions the data controller and/or processor will need to make sure that they have legal basis for data processing. It is unrealistic to expect that in the span of one hour the victim's consent is sought three times, in the detail and under the scrutiny that the GDPR outlines for the consent to be considered valid. Asking a – highly traumatised – victim to undergo this approach is likely to cause secondary victimisation.

This would mean that at the intake point, while victim support organisations cannot fully anticipate what the victim may need in terms of future referral unless an individual assessment is carried out, full consent must be obtained to cover any use of the victim's data as required by the GDPR.

Not only is this approach less than ideal from a victim perspective, but there are also administrative burdens to be considered. Victim Support organisations, particularly NGOs, are underfunded and often have long waiting lists. The additional burden of this lengthy consent process when applied to large numbers of victims would simply mean that fewer victims will be able to receive support. This is significant when organisations have not received additional funding to cover the costs of implementing data protection rules.

Using consent, within the context of victim support, as a basis for data processing is far from ideal.

CASE STUDY

A highly traumatised victim of domestic violence calls a 116006 helpline to seek advice on how to protect herself and her small children.

To provide appropriate information, the helpline worker needs to collect some personal data, including her name, address, phone number, children's ages and names, and details about her employment, family life and social networks.

Before asking any of these questions, the helpline worker is given a script to read to the victim, to ensure that the victim understands the GDPR implications of data processing and to be able to give informed consent. The script is about 2 pages long, is very technical and takes about five minutes to complete. Several times during the reading of the script, the helpline worker needs to insist that the victim repeats certain statements, to ensure that consent was freely given.

Four minutes into the call, the victim hangs up as her abusive partner came back home. She decides that she will never call the helpline again.

Contract as a legal basis for data processing

Some victim support organisations may have a practice of establishing a contract to define the type and scope of services, which are provided to the victim. Some professionals, such as psychologists, use a contract as standard practice. Such a contract can serve as a basis for dat a processing, if the data is collected and used towards the execution of the contract.

Depending on the circumstances, it may be argued that even where there is no document titled 'contract on providing victim support services', the provider and client are entering a contractual relationship. For example, when buying a product online we implicitly agree a contract, and to execute the contract, the seller needs our personal data, which they can ask for under this legal basis.

The same may be argued for some types of victim support services. If a victim calls and asks for a support worker to accompany them to a trial, it is reasonable to require their name and details about the trial (the time, date, specific location), to know where and when to send the support worker.

In this regard, contract, like consent, needs to be an expression of free will and informed decision by the victim.

Legal obligation

A legal obligation to provide a certain service may be a basis for data collection and processing if the data itself is essential to that obligation. For example, in the implementation of court orders, supporting vulnerable victims, such as children, or when support organisations implement a legal requirement. Similarly, a financial institution may be legally obliged to collect the personal data of victims of banking fraud and thus have a justification to process that same data.

To claim legal obligation, the organisation must establish that it has a specific duty to a specific victim. General statements cannot be used as justification. However, this basis cannot be exercised if the support organisation has discretion in whether to process personal data or use another means to comply with the legal obligation.

Vital interest

Some elements of victim support might be considered as acting to protect victims' vital interests, in cases where the lives, or health, of the victims or others are at stake. For example, taking the contact details of a highly traumatised victim to follow up on their wellbeing, even if support had been refused immediately after the event.

Notably, evidence suggests that many victims of terrorism, who have not suffered serious physical injuries, will refuse support at first. However, after the initial shock has worn off, they may feel the traumatised and seek out help. Taking this into account, arguably it would be in the vital interest of the victims to keep their phone number and make follow up calls in the days or weeks afterwards.

Legitimate Interest

Victim support organisations may rely on **legitimate interest** if there is a clear benefit to a data subject (victim) and to the organisation resulting from the data processing; when there is a compelling justification for the processing.

The legitimate interest basis is the most flexible of the legal bases provided by the GDPR. It may be useful to rely on legitimate interest when it is difficult to obtain consent from data subjects and where the impact of data processing on victims' privacy and data protection rights is minimal.

Legitimate interest is not a blanket legal basis for every instance of data processing - GDPR insists that the individual circumstances must be taken into consideration. However, each time personal data is collected, victim support workers will have to carry out a detailed data processing impact assessment.

To apply legitimate interest, a three-step test is recommended:

- **Purpose – is there a legitimate interest behind the data processing? Arguably, the organisation has a legitimate interest to support victims of crimes based on the Victims' Rights Directive and applicable domestic legislation.**

- **Necessity – is the data processing necessary for the purpose. Normally yes, as we need to understand who the victim is and what they have gone through to be**

able to support them appropriately. We need to collect and process their details to help them.

- **Balance – is legitimate interest overridden by the individual's interests, rights, and freedoms? This would rarely be the case, as the data processing is in the individual's interests and is to ensure their rights and freedoms are implemented.**

However, the purpose of the data processing must be clearly explained, and necessity must be demonstrated. To justify the use legitimate interest, a victim support organisation must balance this basis against the data subject's fundamental rights and freedoms.

Given the mission and activities of victim support organisations, this should not be a difficult exercise. Nevertheless, it is important to pay attention to these processes, justifications and reasonings to ensure that reliance on the legitimate interest basis is GDPR-compliant.

CASE STUDY

A young man calls a victim helpline, explains his situation (subjected to a violent attack – possibly hate motivated), and agrees to make an appointment for further help.

To make the appointment, Organisation A records personal data including the victim's name and contact information, details of the crime, and his request for assistance. This information is passed to a local branch, which contacts the victim to book an appointment.

In this instance, legitimate interest is used as a legal basis for data processing. However, it would be good practice to inform the victim, in some detail, how their data will be processed and used, and to let them know how to ask for their data to be removed. They should also told where to find the organisation's data protection policy.

A young man calls a victim helpline and explains his situation. He wants some basic information on his rights but does not want to make an appointment. The VSO took some initial personal information to facilitate their helpline support.

However, the VSO has a policy to recontact victims of violence (as in this case) after 1 week to check if the victim is ok and if they would like any further assistance. All information on the case is retained to enable the follow up contact.

- **Question:** Is there a legitimate interest for processing the data? Does the organisation need to obtain consent to retain, process and recontact the victim?

Answer: Yes, it may be justified that legitimate interest exists to keep the data and call the victim later, but it will depend on the circumstances of the case. Violent crimes can easily justify legitimate interest, and can be claimed when victims are vulnerable, or when other circumstances justify the need to retain victims' data for a certain period. The case worker would need to assess whether legitimate interest is justified or not and make an affirmative declaration to that effect in the casefile for each individual case. This exercise does not have to be too complex, the caseworker may have to answer several multiple-choice questions, but must provide sufficient basis to retain and process the data.

It would, however, be good practice, to tell the victim in advance that he might receive a call the following week and to give him the opportunity to refuse the follow-up. As above, further good practice is to inform the victim about data retention and deletion principles and tell him where to find the data protection policy.

Public interest

If a victim support organisation is entrusted with a task to be performed in the public interest or because it is an official requirement with a clear basis in law and would implicate processing data of victims or other persons, it may use this as a legal basis for lawful data processing[5]. In this case, the data controller (victim support organisation) must demonstrate that the task is in the public interest.

The provision of support, assistance, and services to victims of crime may be considered tasks performed in the public interest. The relevant recital (41) GDPR clarifies that this does not have to be an explicit statutory provision if the application of the law is clear and foreseeable. However, for clarity and simplicity either the organisation or the delivery of support, assistance, and services to victims of crime is described in national law as public interest tasks.

This legal basis for lawful data processing strongly depends on applicable national laws and, in the absence of transparency, interpretation of them by the national data protection authority.

Some elements of victim support, if data is processed to ensure the wellbeing of vulnerable victims or to ensure public safety, can be justified by public interest.

- In the Netherlands, the Minister of Justice issued a ministerial regulation, appointing Slachtofferhulp Nederland as the coordinating legal entity for the support of victims of crime in the Netherlands. Guided by this regulation and its wording, Slachtofferhulp is considered to be acting in the public interest when staff provide support to victims of crime. This is additionally reaffirmed by the fact that victims of violent crimes in the Netherlands are automatically referred to the support services by the police. Through this referral some of the victims' personal data (name, phone number, address) is transferred to support services by the police – arguably in their exercise of a public interest activity when they respond to a report of a crime.
- Slachtofferhulp Nederland also helps victims of traffic accidents. These victims are not mentioned in the ministerial regulation or in law, which means that the public interest basis is more difficult to justify. As a result, other legal bases are used, usually consent.

The argument that victim support services in Europe are of public interest has been reinforced in recent months. From a practical perspective, victim support organisations have been critical to social functioning in the wake of the Covid-19 pandemic. At the national and international level, there have been regular demands that support services remain open, that they receive additional funding to cope

[5] It is also important to note that if data processing is based on the legitimate interest, the public task or authority basis, the data subject should have the right to object to data processing on grounds relating to his or her situation in accordance with Article 21 GDPR.

with Covid-19 related crime issues and to allow them to continue operating under lockdown restrictions, they be recognised as essential services. This approach has been adopted in several countries.

Additionally, the European Commission has recognised the importance of victim support organisations and has called on Member States to recognise them as being essential.[6] This move is important, in view of the increase in certain types of crimes, in particular domestic violence and the increased need for support services for victims.

SAFELY STORING VICTIMS' DATA

As well as the question of whether data is personal and whether there is a legal basis for processing it, personal data must be stored securely.

There are two main approaches to data storage: on paper and digitally. Personal data that is recorded on paper – forms, documents, medical files etc., should always be stored in locked rooms or cabinets. While GDPR does not apply to such data processing, it should be considered good practice to have a safeguarding policy as to who can access paper databases and under what conditions.

Digital data must be protected and organisations must be able to show that they took reasonable measures to keep it secure. Access to data can be password protected or another system can be used to ensure access is limited to only those, who have a justified interest in the data. However, data protection professionals suggest that victims' sensitive personal data should always be encrypted[7]. There are three main approaches to encryption:

Service providers may opt for **local, on-premises storage of encrypted data** on servers kept within the organisation's premises. Hardware for servers will be required, the servers should be kept in an area with limited access – usually a locked server room, and organisations must budget for professional server maintenance.

Alternatively, data can be kept in **cloud storage with server-side and in-transit encryption.** Here, a trusted cloud provider must be identified to encrypt client data and store it, with the corresponding encryption and decryption keys, in a secure place. In this instance, the provider will decrypt data at the request of an authorised person. Such services are offered by almost all cloud providers: Google, Dropbox, Microsoft, Amazon, etc.

From the experts' perspective, the safest way to store sensitive personal data is through **cloud storage with client-side, end-to-end encryption.** The service provider encrypts the client data on their side and stores the encrypted data in the cloud. The service provider, not the client or cloud provider, has sole access to the decryption key. This type of encryption is offered only by a limited number of vendors (for example MicroSoft[8]) and the benefit is that even if the authorities demand access to the victim's data, the provider is unable to hand it over as they do not have the encryption key.

[6] EU Strategy on victims' rights (2020-2025): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0258&from=EN

[7] For more information about encryption, see e.g. https://www.internetsociety.org/encryption/what-is-encryption/?gclid=EAIaIQobChMIj8r86NK_6gIVFOh3Ch2Q4wwBEAAYASAAEgIl6_D_BwE

[8] https://azure.microsoft.com/en-us/services/azure-dedicated-hsm/

Image: Safety ranking of encryption options.[9]

To appraise the best solution for data storage, victim support organisations should conduct a risk assessment exercise and decide the level of protection to go for. There is a saying that there is no 100% safe way to store data, but some approaches are riskier than others.

While in depth analysis of these risks is outside the purpose of this paper, the following risk matrix may be used in identifying prerequisites for managing risks[10]:

[9] Image credit of: https://www.eenewseurope.com/design-center/client-side-vs-server-side-encryption-who-holds-key/page/0/1

[10] Image credit of: Deloitte Privacy Knowledge Center, Data Protection Officer Course, October 2020

CONTROLS	Physical	Administrative	Technical
PREVENTIVE	• Physical security perimeter • Physical entry controls	• Information security, awareness, education and training • Policies and procedures • Notices • Engaging of a subcontractor to process personal data • Contact with authorities	• Information backup • Management of privileged access rights • Inrusion prevention software (IPS) • Segregation of duties • **Cryptographic controls**
DETECTIVE	• Securing offices, rooms and facilities	• Internal audit • Third party audit	• Protection from malware • Logging and monitoring
CORRECTIVE	• Protection against external and environmental threats	• Breach notification • Reporting information security events	• Segregation in networks

Ultimately, EU rules still leave organisations in a state of uncertainty. If they do not put in place the maximum protection possible, rather than what is perceived to be reasonable, there is no guarantee the safeguards will be accepted. This is a challenge for NGOs, which have limited resources and seek to use those resources on their core task of supporting victims.

DATA PROCESSING BY VICTIM SUPPORT ORGANISATIONS

Data processing by victim support organisations should, as discussed previously, not only be guided by GDPR, but also by the need for confidentiality of services and respectful treatment of victims.

A victim support organisation should ensure that:

- **Only data necessary for the provision of a high quality service is collected;**
- **Only support professionals and those organisational staff needing to retrieve personal data to support a victim or perform their professional duties have such access;**
- **Access to data is only allowed when necessary and must be recorded;**
- **Data is processed and shared (both internally and externally) only when it is to benefit of the victim or to comply with statutory obligations (for auditing purposes, etc.);**
- **Data is securely stored while the victim actively receives support from the organisation and then for a predetermined period of time, of no longer than 5 years, after their file has been closed;**
- **Data is deleted at the end of the above period, or as soon as victim requests their data is removed.**

Personal data can be anonymised by support organisations, and kept as such for an indefinite period, for statistical and reporting purposes.

RIGHTS OF VICTIMS AS DATA SUBJECTS

Victims have certain rights in their capacity as 'data subjects'. Details of these rights must be included in the information provided to them, such as **the right to lodge a complaint with a supervisory authority.**

Regardless of the legal basis a victim support organisation uses, it must comply with the duty to **provide information about data processing** under the GDPR. This means that there is an obligation to inform the victim about:

- **whether, and how, their personal data is processed;**
- **the legal basis for data processing, even when in public interest,**
- **the period for which personal data will be stored,**
- **the right to request information about their data and its processing by the VSO,**
- **who it will be shared with[11]; and**
- **the right to demand rectification of incorrect data entries.**

This information can be given in a several ways. Usually, it will be most effective to combine different methods: in conversation during the intake process, in written form by giving the victim a leaflet, and by providing a transparent online privacy and data protection policy.

Additionally, victims should be informed about those **subjects who will potentially receive their personal data.** Whenever possible, this information must be detailed – precisely indicating those entities that will receive the data. When this is not possible, the organisation may provide the categories of recipients. However, the victim support organisation/data controller must explain why specific details cannot be given.

In the context of victim support, a justification will be that it is not possible to know, before an individual assessment, what type of further support a victim might need and who exactly will be able to provide the support. Under such circumstances, the information on the categories of recipients should be as specific as possible, indicating the type of recipient (by reference to the activities it carries out, for example the data processors), the industry, and their location.

For example, if legal aid can be provided through pro bono cooperation with several law firms, victims may be given the list of law firm names and links to their respective data protection and privacy policies.

Victims have the right to know whether and how their personal data is processed, to

[11] Complete list of information that must be provided to a data subject may be found in Article 13 GDPR

seek a copy of their data held by the support organisations and to **demand rectification** of incorrect data entries (Article 16).

Victims also have the right to demand removal, erasure, of their data, which is stored and processed by the victim support organisation, the so-called **right to be forgotten** (Article 17). This right is not absolute and is applicable only under a limited number of circumstances[12], such as:

- **the personal data is no longer valid for the purpose for which it was collected;**
- **data was collected based on consent, which has now been withdrawn;**
- **data was processed on the basis of legitimate interest, which is being disputed;**
- **data was processed unlawfully; or**
- **erasure is required by law.**

In addition to erasure, victims have the right to demand a **restriction of processing** of their data, in which case, the victim support organisation can retain and store the data. The organisation can only process such data with a victim's explicit consent, the data subject's consent (if it is not the victim – the offender, etc.) or for the establishment, use, or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest (Article 18). The restriction of processing is a temporary measure. When a restriction to process data exists, case-management systems should provide an option that clearly highlights restricted victim data and disables processing such data for the duration of the restriction.

Finally, victims have the **right to data transferability** – which means that a victim can demand the support organisation to transfer their personal data to another service provider, where technically feasible (Article 20).

DATA RETENTION

It may be especially difficult for victim support organisations to determine how long victims' data should be stored. While GDPR does not set a time-limit, personal data must be stored for the shortest time possible. The retention period should be used to consider the reasons why a victim support organisation needs to process the personal data as well as what legal obligations apply to storing the data for a fixed period of time (for example, national labour, tax or anti-fraud laws requiring the storage of personal data for a defined period).

A victim support organisation may maintain contact with a victim for an unstated period, and if the contact is maintained, a victim's personal data may be stored. The personal data may be further stored for an additional period: for example, to complete and supplement statistics, to receive feedback on quality of services, etc., are all legitimate reasons for data retention.

- It is important to keep in mind that in cases where support is provided through a network of victim support organisations, which retain separate legal personalities, the victim is, for the purposes of GDPR, being referred to external service provider.

[12] There are some other situations where erasure would be possible, however they do not appear to be relevant for victim support services and are hence not being mentioned here.

It should be emphasised that the main purpose for victim support organisations to collect, store, and share victims' data is to reduce secondary victimisation. If consent is seen as the principal, if not the only, legal basis for storing and processing victims' data and if it is strictly applied every time the victim contacts a support service there is an increased risk of secondary victimisation.

Once the retention period expires, the personal data should be deleted or anonymised for statistical purposes. This can be done through the process of pseudo anonymisation – the data is then no longer attributable to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to prevent the personal data being linked to an identified or identifiable person. For example, personal data (name, address, employment details, etc.) can be replaced by a random code or made-up names.

- The retention period can depend on the circumstances of the case and the prospect of an extended need for support. Victims may return for additional support even years after their first contact or may benefit from follow-up after situations likely to cause re-traumatisation. Of course, organisations can start a new case file when a victim returns, but this can harm the victim as they will have to repeat their story. A support worker will be able to achieve a better connection and establish trust with the victim more quickly if they can refer to archived information of the case even where they didn't work on it. This effectively indicates to the victim that they haven't been forgotten.

  For example, some victims of terrorism associations contact those caught up in previous attacks to check up on them and any possible re-traumatisation they might experience in the event of a new terrorist attack, even years after their own victimisation. To be able to do that, their data retention rules should enable them to keep victims' personal data on file.

  This would suggest a good justification for keeping data, at least for some victims (those likely to experience long term effects) for a longer period – established individually for each such victim.

GDRP COMPLIANT REFERRAL TO SPECIALISED SERVICES

There are three key ways in which victims initially access victim support services:

- **On their own initiative, having prior knowledge of the service;**
- **At the suggestion of the police or other external actors (judiciary, health professionals etc.), who encourage victims to contact victim support services and who may provide victims with information on where to find such services;**

→ **Through referral, where authorities are empowered to collect victims' data and to request victim support services contact the victim.**

Many victims will receive the support they need through a single contact with the victim support service. For others, an individual needs assessment may indicate that the victim requires further support, either internally in the victim support organisation, or through external referral to other organisations/institutions.

Referral should be carried out directly between the referring and receiving organisations, in consultation with the victim. Once an individual assessment indicates that the victim needs further support, the support organisation will identify an appropriate provider of the specific

service, forward the victim's data to the provider and inform the victim of the next steps. In turn, the new provider will directly contact the victim, explain what their services are, and will offer assistance. This referral process, carried out in collaboration with the victim, tends to have a higher victim take up rate than a victim being solely provided information and being left to contact an organisation themselves.

For example, if a victim needs legal representation, the support worker should contact a law firm or a lawyer. The victim's data related to the circumstances of the crime, which are required for the provision of legal services, and any of the victim's vulnerabilities that would affect any phone calls from the lawyer, are shared. The lawyer can then contact the victim directly to request more details or documents and to make an appointment.

However, this is only possible if appropriate data protection and data sharing protocols are in place. Moreover, with respect to the initial referral, when a victim is referred to a victim support organisation for the first time, by the police etc., most successful referral systems are those termed **opt-out,** as opposed to opt-in.

With the opt-out system, a victim is told that their information will be automatically passed to service providers unless they expressly disagree. With the opt-in system, the victim is asked to agree to their information to be passed on, and only if agreement is given does the referral happen.

Whilst the opt-out system seems to produce a much higher take up of services, since GDPR, services are more reluctant to rely on the opt-out for fear of being non-compliant. This is largely due to misunderstanding that compliance is primarily ensured through consent and that it would be non-compliant to pass on victims' data under other legal bases.

A victim should be told about the type of data being shared, with whom, under which conditions, and for which purposes. However, this information can be presented in several ways and it does not mean that specific consent should be collected for every single possibility.

The list of third parties with whom the data may be shared should be included in a privacy notice and periodically updated. it is crucial that a data subject can identify the controllers and the processors of their personal data. This information should be given to the victim the first time their personal data is collected through the provision of a printed list, or by sharing a link with the victim, telling them why the list is being given and what the likelihood is of their data being shared.

Sharing personal data with third parties based on the legitimate interest criterion could be contested by the victim concerned. The legitimate interest basis is used when victims may reasonably expect that their personal data will be shared, for example with the legal aid provider in civil proceedings, and when victims understand how their personal data will be used. Whether a victim truly understands the way his or her personal data is processed and may be passed onto a third party is subject to question and may be situation-specific.

It is important to note that a victim support organisation should have a written agreement in place with any third party with whom it shares personal data. It is also important to review the privacy policy of all third parties and that these policies contain:

- The processing subject matter;
- The processing duration;
- The processing nature;
- The processing purpose;
- The type of personal data to be processed;
- The categories of data subjects;
- The rights and obligations of the data controller;
- Specific instructions in case data is shared with another data processor.

CROSS-BORDER REFERRALS, INCLUDING OUTSIDE THE EU

The same principles for EU cross-border referrals apply as in the case of domestic referrals between service providers. However, if a referral, or the sharing of personal data takes place across borders outside the EU, the data may only be transferred to a jurisdiction[13] or if a victim support organisation has implemented a lawful data transfer mechanism.

For example, the transfers are permitted if the controller or the processor cites appropriate safeguards in the form of Model Clauses approved by the European Commission or national data protection authorities. The transfer may take place based on an approved Code of Conduct, together with binding and enforceable commitments to provide appropriate safeguards.

One may obtain certification for the transfer of personal data outside the EU. This certification, along with binding, enforceable commitments from the non-EU victim support organisation sharing the personal data, guarantees the security of the data transferred. The personal data may also be transferred on the basis that the data subject, having been informed of the possible risks to such transfers, explicitly consents. Other legal bases may be applicable.

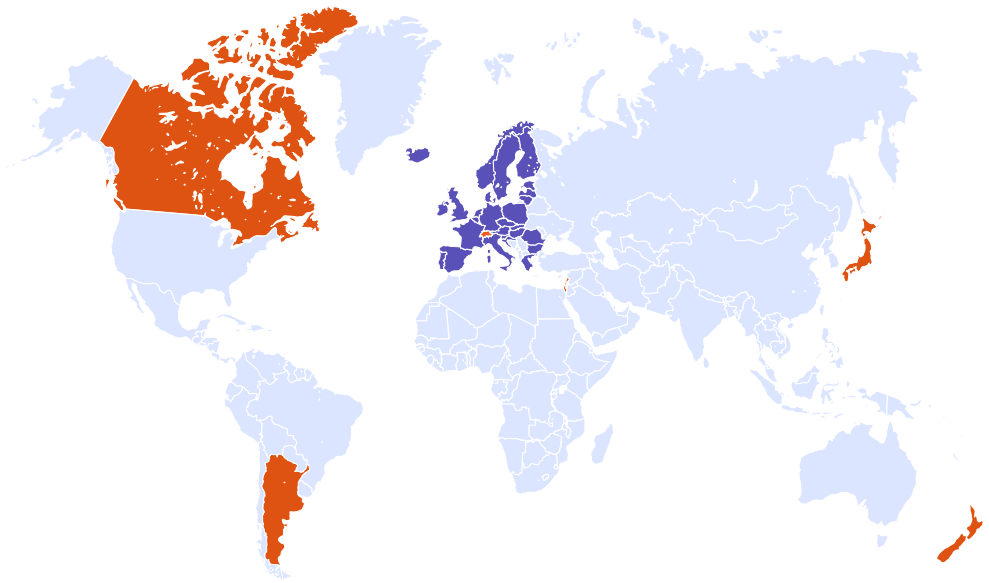
According to the latest information, only a small number of non-EU countries, as presented in the map below are GDPR compliant[14]:

[13] Adequacy Decisions are subject to a periodic review, at least every four years, taking into account all relevant developments. The Commission can repeal, amend or suspend Adequacy Decisions for jurisdictions no longer ensuring an adequate level of data protection. See **https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.**

[14] Image credit of: Deloitte Privacy Knowledge Center, Data Protection Officer Course, October 2020 Also, note that the UK might no longer be compliant after the expiry of the transitional period in January 2021

DATA TRANSFERS

International data transfers



Allowed:

- transfers to EEA countries
- transfers to countries with adequate level of protection

Not allowed without additional guarantees :

- transfers to all other countries

To ensure compliance is achieved, when data is transferred to other countries, there should be a specific agreement with the entity in the non-compliant country, based on the model clauses proposed by the European Union or on binding corporate rules (BCRs) – although the latter are only recommended for complex corporate structures. The list of model clauses is freely available and translated into all EU languages[15].

SPECIAL CATEGORIES OF DATA AND CRIMINAL DATA

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing

[15] The full list can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

of genetic data or 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 are considered special categories of data processing and are in general more unusual. Victim support organisations should rely on domestic legislation, and the individual circumstances of the case, if processing special category data. In principle, this data should only be collected when necessary.

It is possible to consider such processing is necessary for reasons of substantial public interest, is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

This may be justified when this type of data is fundamental for determining the type of support to be provided to the victim – a transgender victim of hate crime, who is being referred to a specialist services, or health data, which is needed for theprovision of psychological support.

It may also be necessary to gather and process such data to describe the specific problems groups of victims face – hate crimes against certain ethnic groups, or identifiable support needs for victims with specific vulnerabilities. In each case, the victims need to be informed that their data is being collected and to maintain their data protection rights.

VICTIM INFORMATION SHEET

Based on the above, victims should be given relevant information on how their data is being stored and processed, and what their rights are when their personal data is collected by victim support organisations.

What GDPR information should be given to a victim of crime?

- Contact details of the victim support organisation;
- Purposes for which the personal data is collected (statistics, case-management, referral to other support organisations etc.);
- The type of personal data concerned (name, address, phone number, type of crime, circumstances of the crime, injuries suffered etc.);
- The legal basis for data processing;
- How long the data will be stored;
- Potential recipients of personal data;
- Whether the personal data will be transferred to a recipient outside the EU;
- Information about the rights of data subjects/victims (such as the right to access personal data), the right to lodge a complaint with a data protection supervisory authority, and the right to withdraw consent at any time;
- Where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

CONCLUSIONS AND RECOMMENDATIONS

Privacy and confidentiality are core to the work of victim support organisations. They are intuitive cornerstones of a trusted high quality service, GDPR standards are a welcome reinforcement to this foundation.

Support to victims of crime is an important societal service that engages and protects fundamental rights such as the right to life and justice. EU Member States have a legal obligation to ensure such services are available and accessible to all. Many countries recognise that victim support is so important that providers should remain open, while other services are closed in the face of a lethal pandemic.

Achieving data protection and victim support is a balancing act. It is critical that **organisations working with victims understand their data protection duties and have in place the correct mechanisms,** procedures and training to respect its obligations and protect victims.

Organisations must implement data protection rules without impeding support given to the victims by **using the wide range of legal bases for the processing of data.**

Insisting on the repeated request for consent may be harmful to victims. By asking them to tell their story several times, by asking them the same questions, and by repeating the same explanations, there is a risk of frustrating or potentially harming already traumatised victims.

While **consent is a central element in working with victims,** relying on consent to process their data can be bureaucratic, burdensome, and counterproductive. **Victim support services should therefore be fully aware of all the legal bases and should rely on those, which best suit their situation and minimise victims' burdens.**

Whilst these obligations rest with individual organisations, the **EU data protection framework has not been designed with them in mind. Vague rules** and the broad room for interpretation left to national data protection authorities, has resulted in **legal uncertainty for victim support organisations.**

Overwhelmed by the pressures of limited funding and the increasing support needs of victims, organisations are left anxious about compliance. **The absence of legal certainty and fear of serious consequences can lead to organisations providing fewer services or devoting fewer resources to expensive unnecessary solutions,** just to be 'safe' from ruinous fines. This situation **risks the quality and effectiveness of victim support services.**

The EU, Member States and Data Protection authorities must join forces with support organisations to develop reasonable, balanced solutions that achieve the objectives of both data protection and support of victims.

Using EU co-operation mechanisms, dialogue between EU and national data protection authorities and victims support organisations should establish **clear, practical, and feasible implementation guidance** so that operators are not working against a backdrop of fear.

The EU and Member States should enable support organisations to rely on legal bases most suited to their situation. This should start with **the recognition of victim support providers as public interest services.** Any service that must be made available as a State obligation under EU law and must remain available to all who need it, for as long as needed, is indeed a public interest service.

Moreover, at least some victim support services are provided in compliance with **a legal obligation.** Some are already imbedded in Member State national legal systems by virtue of the Victims' Rights Directive, the Directive on the European Protection Order, or the Countering Terrorism Directive, to name but a few possible sources of legal obligation.

Finally, it should also be recognised that the **processing of victims' data is done in pursuit of a legitimate, or possible vital, interest** when this ensures that victims receive the support they need, for as long as they need it.

Many victim support organisations operate in fear of potential fines for GDPR non-compliance at the expense of victims' wellbeing. A clear operating framework – based on legal certainty must be developed and **sanctions for non-compliance must consider both data protection and victim support objectives,** recognising the vulnerable financial situation of most support organisations. **Sanctions should promote change and improvement, not result in the loss of critical services** or a more ineffecticient operation of those services.

Guidance on **data protection should enable easy, effective access to support** ensuring that **GDPR does not stand in the way of safe referral mechanisms.** Ultimately, the combination of **appropriate data protection safeguards with the possibility of the opt-out from referral should be consistently recognised across the EU as compliant with GDPR rules.**

Victim support organisations across the EU are committed to protecting the data of victims whilst supporting them. They face multiple hurdles and uncertainties, which are costly from time, resource and financial perspectives.

The EU, Member States and Data Protection authorities owe it to victims to simplify rules and help organisations to comply through a clear legal framework relying on the most appropriate legal bases, and with the provision of adequate funding for organisations' data protection mechanisms.

With Financial support from
the Justice Programme
of the European Union

DECEMBER 2020