The new EU Regulation on the protection of personal data: what does it mean for patients?

A guide for patients and patients' organisations

European Patients' Forum • Rue du Commerce 31 • 1000 Brussels • Belgium
Office Phone number: +32 (2) 280 23 34 • Email: info@eu-patient.eu • www.eu-patient.eu

Contents

1. Introduction

In May 2016, the European Union adopted a new Regulation (EU) 2016/679 on the protection of personal data. The European Patients' Forum has actively advocated for a balanced approach to protect patients' privacy while ensuring patient's data can be shared for healthcare and research purposes since the publication of the proposal for a regulation in 2012. The final Regulation provides more rights to citizens to be better informed about the use made of their personal data, and gives clearer responsibilities to people and entities using personal data.

This document outlines what this new legislation means from a patients' perspective and how patients' organisations can contribute to ensuring that patients' rights to privacy, data sharing, and accessing their health data are implemented optimally.

What is personal data?

Personal data is information about a particular natural person that allows, or could allow identifying the person. It is important to distinguish between identifiable data (even if it is key coded) and data that is rendered completely anonymous, as the Regulation applies to the former, and not the later (Recital 36). It may be any information relating to an individual, whether it relates to his or her private, professional or public life. To be covered by the Regulation the data need to be collected and used by someone else (a person or legal entity).

1.1 WHY DATA PROTECTION RULES MATTER FOR PATIENTS WITH CHRONIC AND LONG TERM CONDITIONS

Patients' fundamental right to protection of their health data is an important issue in diverse contexts such as healthcare, including care given through eHealth or in a cross-border healthcare context, and research (clinical trials, clinical investigations, epidemiological research, patient registries…).

On the one hand, health and genetic data belong to the category of 'sensitive data', and benefit from additional protection in EU law. Unauthorised disclosure of personal health information could negatively impact on an individual patient's personal and professional life.

On the other hand, the processing of health data is fundamental for the good functioning of healthcare services, for patients' safety, and to advance research and improve public health. Patients organisations are also gathering and using patients' data in their advocacy or research activities. So being able to use patients' personal data is sometimes important to advance research, healthcare practices or patients' rights.

> *"Whenever issues linked to data protection are under discussion it is all too easy to get distracted from the one simple point that attracted us to the discussion in the first place: the fact that there are many millions of patients across Europe who have unmet health needs. New treatments are only going to come from medical research and the use of patient data will play a crucial role in this."* Nick Meade, Genetic Alliance UK

For the reasons above it is important that patient organisations are aware of the rights of patients in this area and engage in order to ensure that the patients' perspective on data sharing, consent and data privacy are taken into account in healthcare and research. It is patients' data, patients' health and patients' privacy that are at stake.

1.2 WHY A NEW REGULATION?

New technologies are offering a wealth of opportunities to collect, use and share health data more efficiently, e.g. to empower patients in managing their diseases, for research, and to improve the quality, safety, and efficiency of healthcare systems. But they pose new challenges for privacy and data security.

In 2015, a special Eurobarometer on Data Protection showed that most citizens did not feel in control of what happens to their data nowadays.[1] The new Regulation seeks to address this by empowering citizens with more rights and information.

[1] Special Eurobarometer 431 on Data Protection, June 2015 : http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Currently the Directive on general data protection of 1995 is in application until the new Regulation is implemented. it has contributed to harmonising data protection rules in the European Union. However, a new Regulation was necessary to take into account the changes triggered by new technologies, such as the increasing use of internet and electronic means in healthcare and telemedicine.

While the Directive is not directly applicable in Member States who had to adopt provisions in the national law to comply with it – which gives way to more difference in interpretation from one country to another – the Regulation will apply directly to Member States. Apart from specific exceptions in the text of the Regulation where Member States are allowed to adopt further measures, the same provisions apply across the EU. This can be positive for example to facilitate cross border research and cross border healthcare.

Data Protection: A fundamental right

The Charter of Fundamental Rights of the European Union has established the right to protection of personal data as a fundamental right in its Article 8. It means that everyone has the right to protection of data concerning him or her and that processing* must be fair, for specified purposes and on the basis of the consent of the person concerned. Another important part is that it gives people the right to access data concerning themselves and have incorrect information rectified.

*See page 5 (definition of processing)

1.3 WHEN WILL IT APPLY?

The new Regulation will apply from **28 May 2018.**

1.4 IMPORTANT CONCEPTS IN DATA PROTECTION

Below are some important terms you need to know to understand the EU Data Protection legislation[2]:

Data processing: any operation performed on personal data such as collection, recording, organisation, structuring, storage, adaptation, retrieval consultation, use, disclosure by transmission, making available or disseminating, erasure, destruction.

Data subject: The person the data is about. For example, patients are data subject when their personal data are processed for healthcare or research purpose. The Regulation also grants rights to data subjects in order to protect their personal data.

Data controller: the persons or entities (whether public or private) which collect and process personal data. They determine the purpose(s) and means for processing the data. For instance, medical practitioners are usually controllers of their patients' data.

[2] "Processing" and "controller" are also defined more formally in the Regulation see article 4 (2) and (7)

2. How are patients' health and genetic data protected by the EU legislation?

2.1 GENERAL PRINCIPLES

The Data Protection Regulation sets clear principles that apply to all use of patients' data and to all data controllers. These principles, defined in Article 5, are important because if they are disregarded by a data controller, the use they make of the data is not lawful. **They must always be respected by all data controllers**:

Principle	What does it mean?
Lawfulness, fairness and transparency	Data has to be processed in accordance with the European Union and Member State laws, data controllers have to be transparent with patients regarding what happens to their personal data.
Purpose limitation	The data has to be collected for a specific explicit and legitimate purpose and cannot be used for other purposes beyond that. It is, however, considered that further processing for scientific research, archiving or statistical purposes is not incompatible with this principle. So data can be re-used for research.
Data minimisation	It means that data controller should only ask patients information that is needed and relevant for the purpose for which they are collecting data.
Accuracy	Controllers have to ensure that their data is accurate. If it is not, the controller should take every reasonable step to rectify it.
Limited storage	Data can only be stored for a limited period, except for archiving and scientific research purposes.
Integrity and confidentiality	Data has to be processed in a manner that minimises risks to confidentiality and integrity of the data (which means ensuring its consistency and accuracy, as opposed to data corruption).
Accountability	This is a new principle compared to the 1995 Directive. It means the data controllers should not only apply the principles in the law but they also have to be able to prove that they are accountable and respect the above principles, it means the burden of the proof is with them.

2.2 IN WHICH CIRCUMSTANCES CAN PATIENTS' HEALTH AND GENETIC DATA BE PROCESSED?

Patients' health and genetic data are considered as a special category of data called "sensitive data". This encompasses all personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and merit specific protection as the context of their processing could create significant risks. It is forbidden to share such personal data, including patients' health and genetic data, unless it is under one of the grounds cited in Article 9 paragraph 2, encompassed in the table below:

What is "data concerning health"?
"personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status" Article 4 (15)

What is "genetic data"?
personal data relating to the "inherited or acquired genetic characteristics of a person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample" Article 4 (13)

Ground	What does it mean?
If the patient gives explicit and unambiguous consent to the use of their data	It means the patient made an "affirmative action" (for example ticking a box is an affirmative action, while unticking an already ticked box would not be considered as such) to give an indication that they agree with their data being processed. (For more details see part 2.3). **Example:** The informed consent forms for clinical trials often ask patients for their consent regarding the use of their data.
If the patient makes the data manifest himself or herself	If patients make their health information public, then it means they agree to it being used by third parties and thus the data is no longer particularly protected as sensitive data. Interpretation of what making information "manifestly public" means may differ from one Member State to another.

Ground	What does it mean?
	Example: It is important to note that this provision can raise questions when it comes to personal health information made public on the internet (through a blog or social media).[3]
If it is in the patient's vital interest	Consent is not needed in circumstances where exchange of information is vital for the patient but they are unable to provide consent. **Example:** In a medical emergency situation where the patient is unconscious.
For healthcare purposes	The law allows the processing of patients' data (without asking for consent) for preventive or occupational medicine, for the assessment of your working capacity, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems and services. In these cases, an important safeguard is that personal data can only be collected, used or shared by a person subject to professional secrecy. **Example:** if your specialist needs to notify your general practitioner about your health information, s/he does not need your consent to do it.
For public interest in the area of public health	This ground applies if the processing is necessary to protect the population against a serious cross-border threat to health, or ensuring high quality standards and safety of healthcare, medicinal products, or medical devices.
To carry out the right of the person that controls patients' data in the field of employment, social security and social protection law	This gives the right to data controllers to process health information in the field of employment, for social security and to comply with social protection law. In these cases, Member States should have in place appropriate safeguards for patients' fundamental rights and interest. This safeguard is important given that some patients may face stigma or discrimination due to undue disclosure of their condition, for example in the workplace.

[3] The Article 29 Working Party (established by the Directive 95/46/EC has adopted an opinion related to online media networking which further discusses privacy on social media http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Ground	What does it mean?
	Example: it may be necessary to process identifiable health information for social security activities – for reimbursement of healthcare, or if the patient is entitled to a social benefit as a result of their health condition for example. It may also be necessary in the field of employment (e.g. for sick leaves).
Substantial public interest	Each Member State can define what "substantial public interest" means, but has to respect the essence of the right to data protection, and to adopt specific measures to protect fundamental rights.
For other more specific reasons	Foundations, associations or any other not-for-profit body with a political, philosophical, religious or trade union aim can process the data of their members, former members or persons they are often in contact with in the course of their activities, under the condition that they apply appropriate safeguards. Patients' health and genetic data can also be processed in case of any legal claim.
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	In these cases, researchers can use patients' data without asking for explicit consent if they respect Union and Member States law regarding having other safeguards in place in order to respect patients' rights to data protection. Key-coding the data is considered as one of the possible safeguards.

2.3 RULES FOR CONSENT

The new Regulation establishes rules to strengthen citizen's rights as regards the process of consent for the collection, use and sharing of their personal data.

- The regulation explains that consent must be **explicit and unambiguous,** that is to say it needs to be given through a clear affirmative act, it has to be freely given, and be an "unambiguous indication of a data subject's agreement to the processing of their personal data". This can be written, electronic or oral. Silence or inactivity (a pre-ticked box for example) cannot be considered as consent (Recital 32).

- Data controllers –that is to say persons or entities that collect data from people – have to be able to demonstrate that a person has given consent. In other words, the **burden of the proof** is with them (Article 7 para. 1).
- Consent has to be informed: It has to be demanded in **intelligible and easily accessible forms**, using clear and plain language, and be distinguishable from other matters (Article 7 para.2).
- In addition, patients should be informed on how to **withdraw consent** prior to giving it (Article 7 para.3)
- **For children below 16**, parental consent is necessary for the processing of data to be lawful– Member States may decide to lower that age, but not below 13 (Article 8).

2.4 ZOOM ON WHAT IT MEANS ….

In healthcare: In healthcare, the rules on data protection allows for patients' data to be processed as long as the person who does the processing is bound by professional secrecy (Article 9 para 2 (i)). This means that healthcare professionals and healthcare institutions do not have an obligation to ask systematically for patients' consent before they can use it. However, they are bound by all the principles described in point 2.1 (or Article 5 in the Regulation), which ensures the exemption from consent is proportionate and limited to what is necessary for the patients' health and social care.

This greater flexibility in healthcare to use data without consent can be positive in several respects, as it means:

- **more possibility for communication** of data within a patients' healthcare team which is important for integrated care.
- **it is less burdensome for healthcare professionals** if they do not have to obtain consent every time to share data.

In research: Data protection in health research led to debates during the legislative process, in particular regarding whether there should be exemptions from the obligation to always seek consent before using patients' data for research in cases where asking for consent or re-consent is impossible (Article 89).

EPF's position was that although informed consent is a fundamental right and should be the rule, in some cases exemptions to consent for sharing data are needed to make research possible. In these cases, other safeguards need to be in place to ensure patients' rights are upheld. Examples of such cases are available on the "data saves lives" campaign website.[4] In many cases studies, researchers used data collected by healthcare systems or previous studies and re-consenting all the participants would have represented a disproportionate effort, considering safeguards such as key-coding were in place to protect the data.

In the Regulation, there is an option for exemption to consent for research purposes, and if it is used researchers must ensure that technical and organisational safeguards are in places when using patients' data (Article 89 para 1). The safeguards that must be met will need to be specified in Union or Member State law (Article 89, para 2 and 3). One such safeguard mentioned in the Regulation is **pseudonymisation**[5], which ensures confidentiality through key-coding the data to make it almost impossible to identify who the data is about without the key. It also asks researchers to use anonymous data where possible, especially if identifiable data are not needed for the research purpose that they are pursuing. Anonymising data is different from pseudonymised data, it means that it is completely impossible to find the identity of the person from the data at all.

Another interesting fact for patients is that the Regulation mentions the importance of **registries**, something EPF had strongly advocated for given that patient registries can play a key role in advancing knowledge of diseases and treatment. The legislation explains it is lawful to process data for registries (under the scientific research ground) provided researchers or anyone who is running such registries follow the rules and safeguards established by Member States. (Recital 157).

[4] http://www.datasaveslives.eu/case-studies/
[5] Also defined in article 4 point 5

3. What are the rights provided by EU law to patients regarding their data?

The new Regulation seeks to empower citizens with rights to be informed and puts them more in control of their personal data. These rights apply to patients in healthcare. They also apply in research, though in this case there may be some proportionate exemptions defined by the European Union or Member States, as for example withdrawing a patients' data could have consequences on the research results and quality.

What right?	Article n°	What does it mean for patients?	What to watch out for? (limits to this right)
To access one's own personal data	Recital 63 Article 15	• The right to access your own personal data is part of your fundamental right to data protection • The right to access your medical record is explicitly mentioned in the new Regulation • If you request a copy of the personal data being processed by a data controller about you, they have to provide it to you • The Regulation encourages the establishment of remote ways to provide you with access, such as electronic health records • The controller has the right to check your identity before providing you with the data	• The controller can charge a fee for the administrative cost of providing the data when you request it more than once. Article 12 also explains that a fee can be charged when the request for data is "unfounded" or repetitive. • If you provided your data in the context of a scientific research, there may be exemptions to this right (see part 4.1 of this document)
Right to data portability/to transfer your data from one data controller to another	Article 20	• When you have consented to provide your health data, and that it is in a machine readable format (e.g. in electronic form), you can request to receive a copy in order to transfer it to another entity or person, and you can also demand that it is transferred directly for you	• When the processing of your health data happens on another ground than your explicit consent (see part 2.2), this right doesn't apply, which limits it in an important way

What right?	Article n°	What does it mean for patients?	What to watch out for? (limits to this right)
		• It could be positive and encourage controllers (hospitals, doctors) to ensure that data is in a format that can easily be transferred	• There is no firm obligation for controllers to ensure the data is easily transferable
Right to object to the processing of your data	Article 21	Under the new regulation you can object to the processing of your data by a controller under these circumstances: • If the processing happens for a task performed in the public interest (Article 6 para 1(e)) • If the processing happens for the legitimate purpose of the controller (Article 6 para 1(f)) • If it happens in the context of direct marketing	In research, you can object to the processing, unless it is necessary for a task carried out for reasons of public interest (Article 21 para 6)
Right to rectification or erasure of data	Article 16	You can ask for the rectification of inaccurate personal data (e.g. in your medical record) and incomplete data completed.	
Right to erasure (so called “right to be forgotten”)	Article 17	You can have your data erased. This is the so-called “right to be forgotten”. This is especially the case if: • you have withdrawn consent and the data controller has no other grounds for processing your data • if there is no longer a purpose for processing it, in accordance with the principle of limited storage and data minimisation. • if the processing is unlawful in the first place When the controller has made the information public, e.g. online, he has to take reasonable step to ensure other controllers also remove links etc. in order to implement your rights.	There are derogations to your right to have data erased in research and in healthcare. (see part 4.1)

What right?	Article n°	What does it mean for patients?	What to watch out for? (limits to this right)
Rights in case of breach	Article 34	If there is a security breach and your personal data is unduly disclosed, accessed, or destroyed, the data controller should keep you informed about the breach if it is a threat to your rights or freedoms, unless they have taken other measures to protect the data (like key coding the data). They should also inform their national supervisory authority of the breach.	It is important to ensure that supervisory authorities are accurately informed of the threat to rights and freedoms represented by undue disclosure of health or genetic information.
Right to lodge a complaint and to effective judicial remedy, right to compensation	Article 77, 79, 82	• Each Member State has a supervisory authority for data protection. You have the right to lodge a complaint with these bodies in case of breach of your data protection rights, and the supervisory authorities will also provide forms to facilitate the complaint procedure. If the complaint is about a case of cross border data exchange, there will be cooperation between supervisory authorities. A list of data protection authorities is available here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. • You also have a right to "effective judicial remedy": you have the right to have your right enforced by a court of law when your rights are not respected. • If a data controller infringes this Regulation and causes you damage, whether it is material or not, you have a right to be compensated, in this	

What right?	Article n°	What does it mean for patients?	What to watch out for? (limits to this right)
		case you should lodge a complaint in front of a court of law.	
Right to be informed/transparency	Article 13 and 14	The data controllers have an obligation to provide some information to you. They have to provide it in a concise, transparent, intelligible and easily accessible form, using clear and plain language. If they collect the information directly from you, they have to give you, at the time when they collect your health data, the following information: • identity of the contact person or controller, • the purpose for which your data is processed • the period for which the data will be stored • If they intend to transfer the data in another country • If they would like to process your data for another purpose than the original one • Your rights as a data subject In case the data has not been directly provided by you, the data controller needs to give you the above information, as well as information to identify the source of the data and whether this source was publicly accessible, what category of data was collected (e.g. if it is your health data).	There is an exemption, in the case of research, if it proves to be a "disproportionate burden" to provide this information to data subjects. When data subject's requests for information are "unfounded" or repetitive, controllers can charge you to provide this information (Article 12)

4. Key areas to monitor in the implementation of the Regulation

While the data protection Regulation is an improvement on the previous Directive in various respects, patients' organisations should monitor several areas in implementation to ensure patients' rights are respected and to advocate for patient empowerment.

4.1 EXEMPTIONS TO PATIENTS' RIGHTS IN RESEARCH

The Regulation allows the European Union or Member states to adopt derogations to data subjects' rights for scientific research (Article 89 para 2). The rights affected by these exemptions are, firstly, the right to access one's own data, the right to rectification and the right to restrict or object to processing of one's data. In addition, there is an exemption to patients' right to be informed about the use made of their data (Article 14 para 4b), when providing the information is a "disproportionate effort", and for the right to have one's data erased (right to be forgotten) (Article 17 para 3b).

A derogation can be provided by the Union or Member States' law in cases where the use of these rights by patients participating to research would render impossible or impair the achievement of the purpose of the research. Providing patients with certain information can for example be a problem in a blind trial, or it can come at an important cost when it concerns a large number of participants. Restriction or objection to processing of one's data can also introduce bias in the sample of data used.

There is also an exemption to the obligation to seek consent for research under appropriate safeguards, but these safeguards will need to be detailed. Only the example of pseudonymisation is provided in the Regulation (see part 2.4)

Recommendations for patients' organisations:

- To encourage the EU to develop guidelines to ensure that the derogations from patients' rights for research are used only when necessary and in a proportionate way. This would help to ensure that the interpretation of rules applying in research does not differ widely from one Member State to another, as it is important to enable and facilitate research cooperation in the European Union in order to advance health research.

- To ask the EU and Member States to provide clear guidance on appropriate safeguards to be in place when consent of research participants is not sought in order to ensure patients' data and fundamental rights are still protected. While these safeguards can be adopted at Member State level (Recital 156 and Article 89 para 2 and 3), EU cooperation is necessary to ensure patients have similar rights across the EU.
- To ask for these guidelines to be developed with appropriate consultation of stakeholders concerned including patients.

4.2 OTHER PROVISIONS THAT COULD IMPACT PATIENTS' RIGHTS

Several other rules in the Regulation are of concern either because they could potentially limit patients' rights or because they are subject to interpretation.

The first one is the right to **access one's own medical record and health data when they are being processed**. While the Regulation explicitly recognises this right, and even encourages to provide remote access where possible, it sets various potential limits to that right which can prevent patients from accessing their health data. In particular, the Regulation does not make clear that access must be provided for free, and even allows data controllers to charge a fee for administrative costs if data subjects ask for the data more than once.

Recommendations for patients' organisations:

- To advocate for patients' free access to their medical records and health data, as this is important for their health literacy and management of chronic conditions
- To ensure Member States take into account that patients with chronic and long term conditions may need to ask for access to their data more frequently, in order to manage their conditions.
- To report obstacles that patients encounter to EPF and/or decision makers or supervisory authorities
- To encourage the establishment of electronic health records, with the involvement of patients and their organisations.

Another provision of concern is the right of data controllers to process data for employment and social security purposes. While this may be necessary, a key issue for patients in the risk of undue disclosure of their condition to employers, colleagues, or insurances given that they sometimes face stigma and discrimination at work or in insurance and banking. Article 88 allows Member States to adopt more specific rules on the processing of data in the field of employment, including specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.

Recommendation for patients' organisations:

- Raise awareness of decision makers in Member States that patients with chronic conditions can be vulnerable to discrimination and stigma in the fields of employment and insurances
- Encourage decision-makers to adopt appropriate measures through legislation to protect patients' personal health data in this area

In case of data breaches, controllers are only asked to notify the breaches to patients if their fundamental right or freedoms are put at high risk.

Recommendation for patients' organisations:

- Raise awareness of decision makers and supervisory authorities in Member States about the consequences of undue disclosure of health and genetic data on patients' rights and freedoms

4.3 ENSURING PATIENTS' VOICE IS HEARD IN DATA PROTECTION DEBATES

While there are no specific provisions on patient involvement in the governance around data protection, ensuring the voice of patients is heard when it comes to matters of personal data protection, privacy and sharing of data is essential to communicate accurately their needs and preferences to decision makers.

Article 80 of the Regulation provides the possibility to mandate a not for profit organisation with a legal status, and which has "statutory objectives which are in the public interest", and is" active in the field of the protection of data subjects' rights and freedoms" to complain with the supervisory authority on their behalf or seek a legal response from a court. Potentially, depending on a Member State's law and interpretation of these provisions, patients' organisations could be allowed to play this role for patients.

Recommendation for patients' organisations:

- Ensure you inform your patient community about their rights to data protection under EU and national law
- Collect information regarding patients' needs, preferences and obstacles they face in using their rights in this field to inform your advocacy

4.4 WHAT ABOUT WHEN PATIENTS' ORGANISATIONS ARE COLLECTING, USING, AND SHARING PATIENTS' DATA FOR ADVOCACY PURPOSES?

The Regulation on data protection applies directly to everyone that processes data, including patient organisations. Thus patient organisations can be data controllers. It means that you can only process patients' health data on the grounds referred to in article 9, and that you need to respect the principles outlined in part 2.1 of this document. For patients' organisations that run a patient registry for research purposes, the rules described in article 89 of the Regulation apply (they are described in part 2.4 and 4.1 of these documents).

Recommendations for patient organisations:

- Ensure you have the right procedures in place in accordance with the principles in part 2.1 and the rights described in part 3 when processing the health data of patients
- Ensure you provide patients with appropriate consent forms or procedures and information on their rights (including the right to withdraw consent) when needed, e.g. when they provide testimonies that you plan to use in advocacy work.

5. Conclusions

The General Data Protection Regulation provided new or clearer rights to citizens and patients compared to the Directive from 1995, but some of these rights have limitations. Patient organisations have a key role to play in ensuring patients are informed, empowered and involved in this area, to ensure that their right to protection of personal data is implemented while maintaining the possibility for patients to share their data smoothly for the management of their condition by health services, and to advance health research.

Big data is becoming an increasingly important topic in the health area. Big data is the combination and analysis of very large and diverse sets of data in a drive to generate healthcare innovation. It has wide reaching implications for patient care and medicines regulation, for example through the blurring of distinctions between non-health and health data; ongoing generation of information about the real-world use of medicines; patient-generated data from social media and wearable devices, and other issues which EPF will be looking at carefully in the next years. Therefore, it is important that patient organisations' continue to collect and communicate the patients' perspective on protecting and sharing of health data.

6. Resources

- The full text of the General Data Protection Regulation in all the official languages of the EU: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
- The European Commission published a questions and answers factsheet which gives general information the Regulation: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
- During the debate, EPF participated to the Data Saves Lives Campaign alongside other NGOs to raise awareness of the value of health data for research: http://www.datasaveslives.eu/
- The fundamental Rights Agency has published a handbook on data protection (based on the Directive from 1995) to make it more accessible: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf
- EPF's position paper and statements on Data Protection can be found here: http://www.eu-patient.eu/whatwedo/Policy/Data-Protection/

This guide on data protection for patients and patients' organisations received funding under an operating grant from the European Union's Health Programme (2014-2020).

The content of this guide on data protection for patients and patients' organisations represents the views of the author only and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.