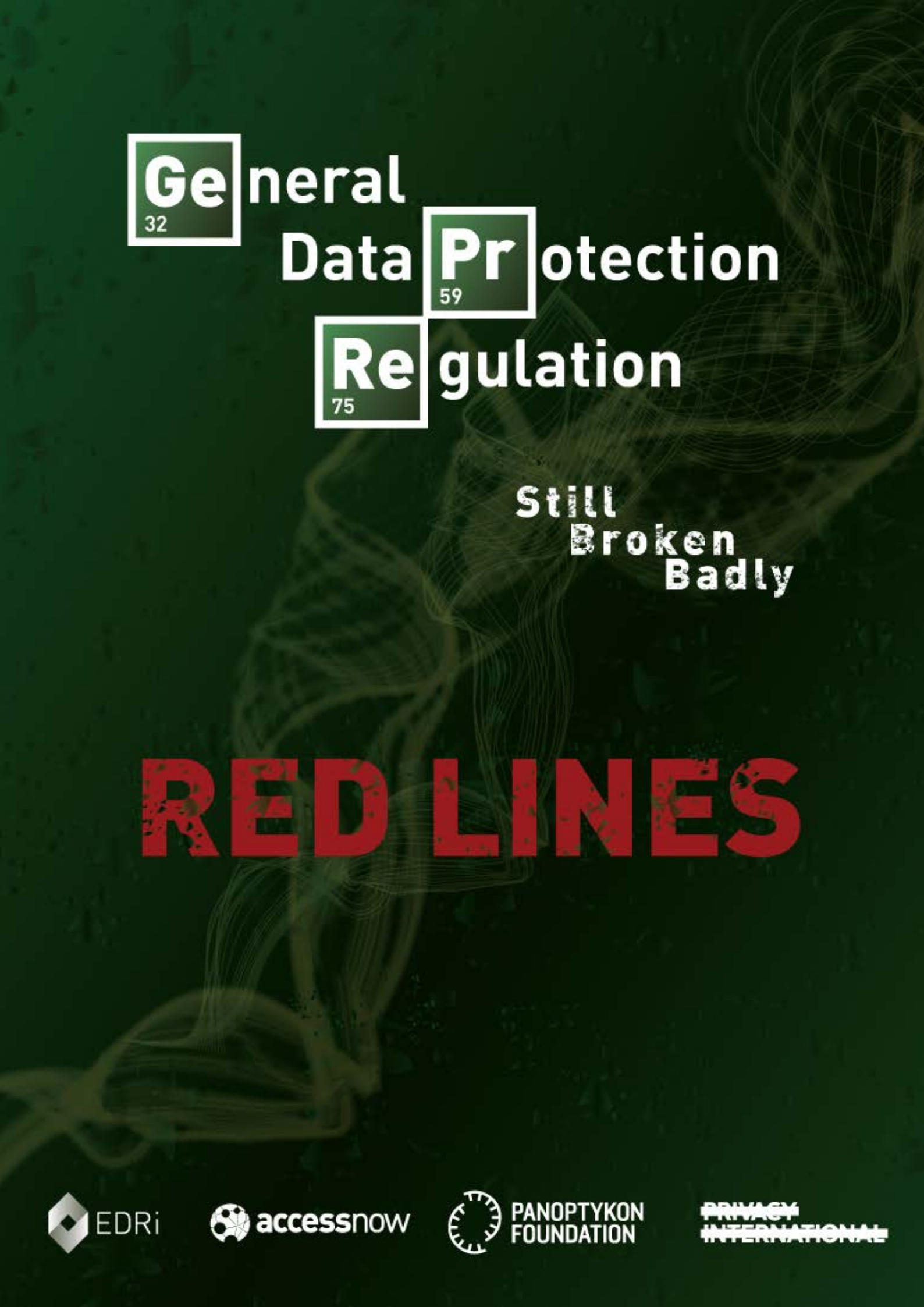

Ge 32 neral
Data Pr 59 otection
Re 75 gulation
Still Broken Badly
RED LINES
EDRi
accessnow
PANOPTYKON FOUNDATION
PRIVACY INTERNATIONAL

As the trialogue negotiations move along, EDRi, Access Now, Panoptykon and Privacy International, would like to provide comments on fundamental elements of the General Data Protection Regulation.

Today, **our personal information is being stealthily collected, shared, stored and analysed everywhere**. Whether you are browsing the internet, talking to a friend or making an online purchase, personal data collection is taking place. We are now at the start of the "internet of things", where more and more devices are connected to the internet, generating still more data. The General Data Protection Regulation (GDPR) is a unique opportunity to improve the EU data protection rules, strengthen users' rights and generate the necessary trust in order to respond to the 21st century challenge.

One thing is clear, **users must regain control over their personal data and companies and states must generate a culture of respect for citizens' rights to data protection and privacy.**

The principles of data protection are the foundation on which the right to our personal data is built. If the principles are weak, then the entire structure will be weak and unreliable. It is essential for the individual to know:

1. who is collecting his or her data
2. that only the necessary data can be collected and,
3. that the purpose of collection is specified and limited.

These principles give a degree of predictability and control to the individual. In short, **data may only be processed when it is necessary and the processing is done for specific and clear purposes**.

OUR RED LINES FOR THE ONGOING TRIALOGUE NEGOTIATIONS

Let's not be ambiguous: Consent need to be explicit

In 1990, the Commission proposal for a Data Protection Directive established that consent should be "expressly given". After several years of negotiations, the Council decided to use the word "unambiguous" to define consent while stating that this wording "does not lead to any lowering of the level of protection". In fact this term is quite ambiguous: for example consent could be inferred from a number of unrelated actions, such as browsing a website.25 years later, we find ourselves having the same debate. Let's not be ambiguous anymore: consent needs to be explicit!

Google Archives are not the National Archives

Article 83 defines the rule for the use of data for statistical research and scientific-historical purposes. Back in 1995, the only research institutions that carried out such activities were probably the national statistics offices of a State research, but the situation is much more complex nowadays. A large number of private companies conduct "research" or even have a business model based on the statistical analysis of vast amounts of collected personal data, so-called big data. These newly developed activities should not fall under the scope of Article 83 to avoid foreseeable abuses of users' data protection rights. We therefore recommend limiting this exception to research activities conducted for the public interest.

Facebook's and others' "legitimate interest" to know everything about you

Article 6(1)(f), allowing the processing of data for the purposes of the controller's legitimate interest can in practice offer controllers a way to circumvent consent restrictions on processing altogether. Current experiences suggest that few data subjects will be able to challenge company practices based on this criterion in court. Moreover, the broadness of the term "legitimate interest" creates legal uncertainty, both for data subjects and business. This criterion for processing data is unfit for the current digital economy, and

must be subject to strong safeguards, with obligations on controllers much more tightly defined to ensure that data subjects are placed at the centre of this reform and that they are able to regain control over their personal data. Anything less is a missed opportunity.

No further processing in case of incompatible purposes

The proposed article 6.4 goes against the basic data protection principle of purpose limitation. It must therefore be deleted.

Turn on the flashlight, it needs to check who your friends are

Article 7.4 needs to include the prohibition of tying, which would make impossible to oblige to give consent to unnecessary uses of your data. As one of numerous examples, there is no need for mobile phone flashlight application to require access to your contact list. Therefore, consent must be purpose-limited.

Empower the data subjects!

Information about the procedures and mechanisms to exercise their rights should be given to data subjects in writing and, where possible, in electronic form. This information should be available free of charge and in simple, clear language. Information rights must also cover profiling measures and should include a mechanism to enable the data subject to exercise his or her right to erasure.

Data protection by design and by default

The implementation of data protection by design and by default are essential. This means procedural and technological means of protection need to be built into any service where personal data is used and that the default setting must offer the highest level of protection for individuals' personal data.

Specifically, controllers should introduce technical standards at the design stage that will ensure that the processing of personal data will meet the requirements of the GDPR and will safeguard the rights of the data subject as effectively as possible. All technical

standards need to promote built-in privacy protection and favour the wide deployment of privacy-enhancing technologies.

Profiling – one of the biggest challenges of this Regulation

The provision on profiling must take account of two aspects:

1. whether and under what conditions a profile, meaning the linking of personal data to generate new personal data and permit assumptions to be made about a data subject, may be created and further processed, and,
2. under what conditions an automated measure based on that profile is permissible, particularly if the measure is to the disadvantage of the data subject.

So far, the proposed texts only address the second element. Unless profiling is comprehensively defined as mentioned above, it will be impossible to object to the mere constitution of a profile. It is fundamental for legislators to tackle this issue, as profiling practices are developing and spreading rapidly. Both the collection and processing of data for this purpose, as well as the "outputs" need to be rigorously regulated to avoid discrimination and ensure that the future legal framework is fit for current and future challenges.

Currently, profiling is one of the exceptions foreseen in Article 21. Although deleted in the Parliament text, the Council text has re-introduced the possibility of having profiling as one of the exceptions foreseen by the Regulation. Profiling raises serious concerns for the right to privacy and could lead to discrimination if not properly addressed. To avoid the creation of 28 different sets of rules that would put some EU citizens with lower protection that others, this issue must be tackled in the Regulation and taken out of Article 21.

To harmonise or not harmonise, that is the question – The getaway clause for public authorities in Article 21

The Regulation will increase, in Article 21, the number of exceptions in relation to the 95 Directive – and thereby reduce the overall level of protection. The exception which allows Member States to introduce additional exceptions based on a "general public interest" objective is of particular concern. This objective, by definition, will have nothing to do with

the other defined exceptions listed in Article 21 (e.g. any general public interest purpose will not be associated with national security; defence; public security;the prevention, investigation, detection or prosecution of criminal offences) and could be used for a vast variety of purposes, becoming a major loophole in the Regulation. In addition to its scope being narrowed, independent review of any such exceptions by the EDPB would be a useful safeguard.[1]

No double standards: EU data protection rules need to apply to EU institutions

The creation of a new comprehensive data protection framework is the right moment to get EU institutions under the same regime. So far, the EU institutions needed a specific Regulation as a Directive cannot apply to their activities. This will no longer be an issue with the GDPR, therefore the scope of application of the Regulation should include the EU institutions.

Adapting Chapter V in light of the Safe Harbor ruling

In light of the recent ruling in the Schrems case, some of the provisions of the Chapter V on data transfer discussed during the first trialogue meeting back in July should be reviewed.

Article 41 on adequacy mechanism must introduce the reference made by the Court that "adequate level or protection" means "essentially equivalent".

The Safe Harbor debacle has proven that the decision to approve data transfer to third countries cannot be left to the sole discretion of the European Commission. As the Court rightfully pointed out, the Commission was aware of the shortcoming of the EU-US data transfer mechanism and its failure to guarantee sufficient privacy protections and, despite this, failed to act to put an end to such abuses. We therefore strongly encourage the legislators to change all "implementing acts" into "delegated acts" in Article 41 in order to provide a veto power to the European Parliament. The relevant data protection authorities should also be required to provide a binding opinion for the Commission on every adequacy mechanism. Finally, to avoid situation were users rights are infringed for the long duration of the Regulation without the possibility of a comprehensive and periodic review, the delegated acts must be coupled with a five-year sunset clause.

1) For a detailed analysis of the vast amount of exceptions in Article 21, go to http://amberhawk.typepad.com/amberhawk/2015/08/councils-exceptions-from-the-data-protection-regulation-degrade-the-privacy-protection-below-directive-9546ec.html

Codes of Conduct & certification seals in light of the Schrems case

Inclusion of codes of conduct and certification as mechanisms for transfer to third countries are only acceptable provided that:

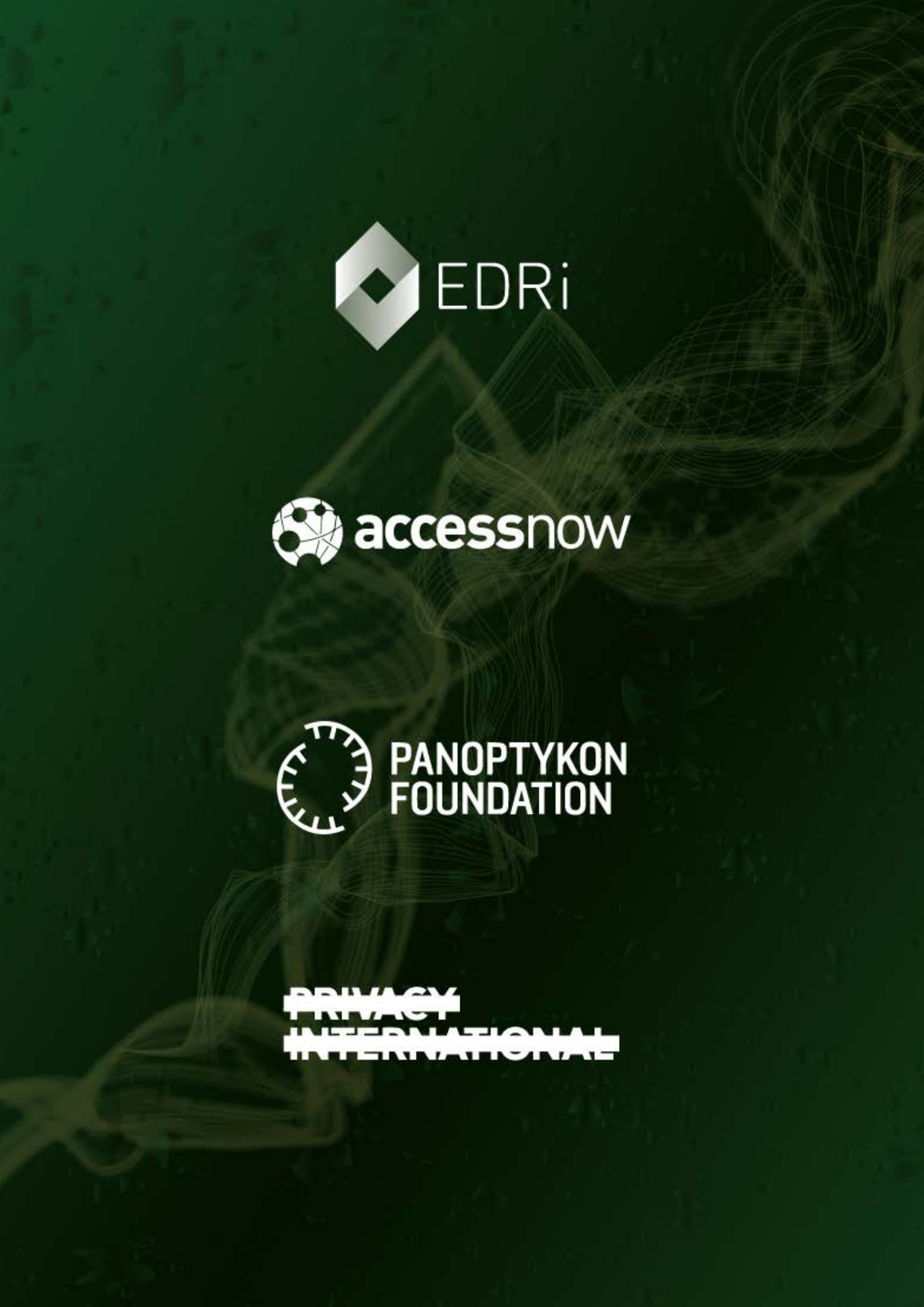
- privacy seals are issued by or under the authority of a data protection authority and codes of conduct are issued or endorsed by a data protection authority;
- such seals and codes are subject to the consistency mechanism; and, equally importantly
- seals and codes will be legally enforceable on those to whom they apply, to ensure implementation, enforcement and redress.

If these safeguards are not in place, the use of codes of conduct and certification mechanisms for the transfer of data outside the EU must be excluded, since they would become huge loopholes in EU data protection standards that would undermine the fundamental rights to data protection and privacy.

Mandatory Data Protection Officer

The introduction of mandatory data protection officers for companies would not only help companies to establish data protection mechanisms in their organisations and to work internally on improvements, but would also bring positive effects for the relationship between companies and their customers by providing a competent contact person for questions related to data protection. Therefore, the designation of a data protection officer for controller and processor must be mandatory as it is suggested by the EDPS in its recommendations for the Regulation (Art. 35).[2]

2) https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf


EDRi
accessnow
PANOPTYKON
FOUNDATION
PRIVACY
INTERNATIONAL