The Single Digital Gateway Regulation as an Enabler and Constraint of Once-Only in Europe

Hans Graux(✉)

Timelex Law Firm, Brussels, Belgium
hans.graux@timelex.eu

Abstract. The adoption of the Single Digital Gateway Regulation is a gamechanger in European e-government. For the first time, it creates a horizontal, non-sector specific legal framework for the direct exchange of digital evidence between public administrations in different Member States. However, these exchanges require public administrations to have a certain degree of trust in each other, which is built on a shared legal basis. The Single Digital Gateway Regulation achieves its goal of creating a legal basis and establishing trust, but also builds in a number of explicit and implicit legal constraints. These will help make the once-only principle in Europe a reality, but also enshrine limitations that will require revisions and expansions of the Regulation at some point in the future. This paper examines the genesis of the Regulation, its legal choices and priorities, the resulting implications and limitations, and potential challenges for the future.

Keywords: Single Digital Gateway Regulation · Legal framework · Trust

1 Introduction on Once-Only Legislation

1.1 Legal Frameworks for Once-Only at the National Level

The once-only principle is not an entirely new concept, and already has a significant policy background in a number of Member States. In each country where the principle has been adopted at some level, legislation was also introduced in order to provide a clear legal basis and scoping of the principle and its effects. The need for such legislation is obvious: as described elsewhere in this book, the once-only principle fundamentally requires that certain information about a citizen or business can be transferred relatively seamlessly from one administration to another, in order to permit that information to be reused, thus relieving the citizen from a tedious burden while increasing efficiency and reducing errors.

These manifest benefits also imply a risk, however. Should the citizen or company be aware of the information exchange? What happens when the information contains errors? Which administrations are actually entitled to request information, under which conditions, and for which purposes? Which sources should administrations rely upon,

R. Krimmer et al. (Eds.): The Once-Only Principle, LNCS 12621, pp. 83–103, 2021.
https://doi.org/10.1007/978-3-030-79851-2_5

and to what extent can the information be expected to be accurate? All of these questions are critical, and answers can differ from country to country.

None the less, some characteristics recur quite frequently in Member State legislation. Typical examples of common requirements include notably:

- An explicit designation or description of authoritative sources (e.g. enumerated in the law or identified through subsequent formal decisions);
- An assertion that those sources are deemed the sole source of specific information (in order to avoid multiple and potentially conflicting databases being queried for the same data);
- A qualification of the information in those sources as benefiting from a presumption of legal accuracy;
- An explicit designation or description of public authorities which can request information from the authoritative sources;
- A legal obligation to request information from those sources – and not from the citizen or business concerned – whenever this is feasible;
- A legal obligation to notify the authoritative source if a gap or inaccuracy in the information is identified, so that the quality of data can be maintained and even improved over time, and to avoid misinformation from spreading.

While not universal, such obligations are generally fairly representative of the legal environment in which the once-only principle is implemented at any given administrative level (federal, national, or regional). The ultimate effect is the creation of a circle of trust between the designated public authorities, in which information can be exchanged with relative freedom without necessarily relying on the citizen or business as a carrier of their own data. As will be described in the following sections, recreating such a circle of trust is both the main objective and the main stumbling block for EU level legislation.

1.2 Scaling up the Law to Cross Border Once-Only

The Single Digital Gateway Regulation is a first attempt at building a European legislative framework for cross-border once-only services (among several other topics). The functional objective is described at a high level in recital (44) of the Regulation, which notes that "*The cross-border application of the 'once-only' principle should result in citizens and businesses not having to supply the same data to public authorities more than once, and that it should also be possible to use those data at the request of the user for the purposes of completing cross-border online procedures involving cross-border users.*" In order to achieve this objective, the Regulation calls for the creation of a "*fully operational, safe and secure technical system for the automated cross-border exchange of evidence between the actors involved in the procedure, where this is explicitly requested by citizens and businesses*".

The elaboration of the once-only principle in the Regulation, including its constraints and prerequisites, can be found mainly in Article 14 of the Regulation, which will be discussed in-depth below. However, it can already be noted that the approach of the Regulation differs significantly from the common elements found in national level legislation as summarised above. Notably, the Regulation does not designate authoritative

sources, nor does it identify authorities that can request information from these sources. The Regulation also doesn't grant exchanged evidence any particular presumption of legal value, other than by noting that the evidence is "deemed to be authentic" – meaning that it should be considered to be originating from the competent authority, without however addressing whether that implies that it is adequate for the procedure at hand. And perhaps most critically: it emphatically places the users – citizens or businesses – at the centre of the once-only principle: as a general rule, evidence is exchanged using the once-only principle at the explicit request of the user.

All of these choices are the result of a delicate balancing exercise. The European Union has no prima facie competence to legislate administrative procedures horizontally, and it arguably would not be proportional to attempt to do so. Indeed, the formal legal basis of the Regulation is the protection of the free movement of citizens, based on Article 21(2) and Article 114(1) of the Treaty on the Functioning of the European Union (TFEU), as indicated in recital 6 of the Regulation.

The Regulation thus cannot directly envisage an overhaul of national public administration, which is one of the reasons why it would not be capable of designating competent authorities or of regulating the legal value of national evidence. None the less, the implementation of the once-only principle implies the creation of a circle of trust, at least to a sufficient extent to allow public administrations to exchange information without relying exclusively on the citizen or business as an intermediary.

At the national level, administrative proceedings can be directly regulated, and obligations – including the participation in a circle of trust - can be imposed directly on the administrations themselves. At the European level, the citizen or business must be at the centre, and therefore the Regulation is drafted in a user-centric manner: exchanges of evidence under the Regulation are generally driven by a user request, and imply prior verification of the evidence by the user. The user decides which exchanges can occur.

As will be examined in greater detail below, this has significant benefits, but also implies some constraints, both in terms of user friendliness and in terms of functionality. Mainly, the requirement in principle of a request and of verification of the evidence by the user ensures that no evidence can be exchanged under Article 14 without the user's awareness and approval. While the benefits of this approach are obvious, it also implies that the Regulation and its technical system will not be useful as devices for detecting malicious or unlawful behaviour: since the user will typically refuse to approve exchanges of evidence which will have negative consequences (e.g. documents proving that they are not or no longer eligible for a specific procedure or service), the Regulation will not be useful for public administrations as a mechanism for catching persons that attempt to circumvent legal requirements. In that sense, the Regulation serves the individual interests of the users more than the interests of the public administrations, or arguably even the public interest. Examples of these choices will be provided in the sections below.

2 The Single Digital Gateway Regulation – Concept and Choices

2.1 General Model for Trust Between Public Administrations Across Borders

Any implementation of the once-only principle implies the creation of a circle of trust between participation public authorities. After all, the principal operational requirement is that one public administration can request information pertaining to a citizen or business directly from another public administration, rather than from the citizen or business itself. While safeguards can and usually will be built in to avoid unlawful access to or use of the information, a mechanism to establish and maintain trust is necessary.

Within the Single Digital Gateway Regulation, this is done through a combination of elements. Firstly, as already noted above, Article 14 requires that the exchanges of evidence occur via a single technical system, which must be "*established by the Commission in cooperation with the Member States*". The development, availability, maintenance, supervision, monitoring and security management of the technical system is a split responsibility of the Commission and Member States, who are each responsible for their respective parts of the technical system (Article 14.11). Since Member States are also explicitly required to "integrate the fully operational technical system as part of the procedures" covered by the Regulation (Article 14.7), the phrasing of the law strongly suggests a federated or at least strongly decentralized model – although this terminology is not used in the Regulation itself - in which each Member States retains a clear degree of control over their national administrative activities, with the Commission operating a smaller central component of the system that will be responsible for interconnecting the national nodes.

Thus, the technical model which is suggested by the Regulation already ensures that each Member State maintains control over national components of the infrastructure. Of course, in order for once-only exchanges to be viable, a more critical question is the trust in the infrastructure of *other* Member States, and in their compliance with the requirements of the Regulation. To some extent this is addressed by the Regulation's reliance on technical and functional "building blocks", which are already in use across the Member States and which offer basic capabilities such as electronic identification (the eID building block) and exchange of documents (eDelivery building block). As the recitals note, "*those building blocks consist of technical specifications, sample software and supporting services, and aim to ensure interoperability between the existing information and communication technology (ICT) systems in different Member States so that citizens, businesses and administrations, wherever they are in the Union, can benefit from seamless digital public services*". On the basis that Member States could be trusted not to modify these building blocks in a manner that undermines their legal value, this already forms a part of the puzzle.

The building blocks are far from sufficient to bring about the entire technical system, and new components – which can form a Once-Only building block in its own right – can be governed by a new implementing act that sets out the technical and operational specifications of the technical system as a whole, as envisaged by Article 14.9.

However, this approach only touches on the trustworthiness of the technical infrastructure. Apart from this issue, the Regulation also imposes a number of functional and design constraints on the way the once-only principle can operate, including the role of

the user, constraints on the use cases and evidences, and procedural safeguards. These will be discussed in the sections below.

2.2 Drawing the Lines: A Closed Model for Once-Only

One of the principal elements to be regulated in any legal framework pertaining to the once-only principle is the scoping of the use cases in which it can or must be applied. At the national level, this is commonly done by identifying the relevant authoritative sources and the public authorities that should rely on them, rather than opting for the definition of specific procedures. At the European level however, that approach would not be feasible, since neither the information sources nor public authorities are organised in a harmonised and homogeneous manner across the EU. In other words, it would not be possible to designate the evidences and the databases covered by the Regulation, or to specify the authorities, since those evidences, databases and authorities may not exist in some Member States, or at least be so incomparably different as to make a regulatory scoping meaningless.

For that reason, the European legislator opted for a different approach. In order to make sure that the Regulation contained appropriate constraints on the cases in which the once-only principle could be applied, even though neither evidences nor authorities can be clearly described, it opted for an exhaustive enumeration of the procedures in which the technical system could be used to support once-only exchanges.

More specifically, article 14 of the SDGR requires that this system supports the exchange of evidence necessary for the completion of the procedures listed in annex II of the SDGR, as well as procedures governed by the Directive on the recognition of professional qualifications, the Directive on services in the internal market, the Directive on public procurement, and the Directive on procurement by entities operating in the water, energy, transport and postal services sectors. Given that the entire list focuses on procedures which are either harmonised through EU level Directives or (in the case of Annex II) which are focused on universal high level "life events" such as birth, changing residence, or retiring, these procedures should indeed exist in all Member States, even if the competent authorities and evidence for each of the procedures might vary significantly.

While the approach has the benefit of feasibility, the downside is the fact that it is a 'closed list' approach, which does not allow new use cases or new procedures to be added without an amendment of the Regulation itself. It would of course also be feasible for future legislative initiatives to explicitly reference the use of the technical system envisaged by Article 14, but in the absence of new regulatory interventions, the growth potential of the number of procedures is inherently limited. This is a constraint that directly results from the impossibility to directly regulate authoritative sources and public authorities at the European level, but the unfortunate outcome is a lack of flexibility when new once-only needs will be identified. The TOOP pilot project already encountered this in one of its use cases, focusing on the exchange of evidences in a maritime environment: while this would be a good target for EU level once-only procedures, it is not included in the Regulation's closed list, and therefore would not be able to make use of the technical system under Article 14.

The scoping of exchanges of evidence is thus limited to specific procedures enumerated in the Regulation. A secondary but related issue is whether, once a public authority has received evidence in accordance with the Regulation through the technical system, they can share it with additional authorities within their own country.

The Regulation does not appear to comprehensively address this question. Article 14 does contain a purpose limitation principle, which notes that "The evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used by that authority for the purpose of the procedure for which the evidence was exchanged" (Article 14.8).

However, the use of the evidence "for the purpose of the procedure" should arguably also include any use of that evidence which is mandatory under national law as a result of that procedure, and which may also involve further use of that evidence. It is likely that some Member States will have their own once-only principles, governed by national law, under which they share data (including evidence) with other public administrations, or under which they are required to retain evidences after receiving them under the SDGR. There seems to be no prima facie reason why the SDGR would invalidate such national laws.

By way of example: after an exchange of evidence under Article 14, the evidence may need to be kept in an official archive under national archiving laws under national legal frameworks. Such uses however are subject only to national laws, which are not affected by the Regulation. As recital (26) to the SDGR notes, "This Regulation should also not affect the procedural workflows within and between the competent authorities, the 'back office', whether digitalised or not". Otherwise, use of the technical system would make it impossible for receiving competent authorities to respect national laws, or at least require them to create exceptions in existing laws to the effect that evidence may be reused whenever their laws require it, except if it reached their competent authorities through the technical system under the Regulation. That approach would likely be unworkable in practice. Thus, it seems reasonable to argue that the Regulation's requirement to only use evidence for the purpose of the procedure for which the evidence was exchanged should not affect further uses that are mandatory under national law. lease note that the first paragraph of a section or subsection is not indented. The first paragraphs that follows a table, figure, equation etc. does not have an indent, either.

2.3 User Centricity as the Principal Driver

It has already been stressed in the sections above that the Regulation takes a user-oriented perspective on the once-only principle, by introducing a general requirement that the technical system "shall enable the processing of requests for evidence at the explicit request of the user" (14.3 (a)). Moreover, it adds that the "use of the technical system shall not be obligatory for users and shall only be permitted at their explicit request, unless otherwise provided under Union or national law" (14.4). Finally, the Regulation requires that the technical system "shall enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence" (14.3 (f)). Thus, three clear elements of user centricity are enshrined in the text: the explicit request, the preview, and the optionality of using the system.

The Explicit Request

Requirements for the validity of an explicit request are outlined in the Regulation, which stresses that it must be "an explicit, freely given, specific, informed and unambiguous request of the user concerned", as a result of which consuming authorities must "request evidence directly from competent authorities issuing evidence in other Member States through the technical system" (article 14.7 SDGR). The technical system for the cross-border exchange of evidence must thus support a mechanism for the user to express an explicit request that meets the requirements above.

The phrasing of these requirements for an explicit request is nearly identical to the definition of a 'consent' in the General Data Protection Regulation. None the less, for reasons that will be outlined below, the concepts should not be conflated: the expression 'consent' does not occur in the SDGR, and the notion of 'consent' should not be used as a reference to the explicit request requirement of article 14 of the SDGR.

This approach puts the user in control over the evidence exchange, which has both benefits and downsides. The benefit (and goal of this requirement) is that the user is protected against potentially unlawful exchanges of evidence without their knowledge. The downside is that the user must in principle be involved in authorising an exchange. A transfer that would be beneficial for competent authorities (or for the public interest) may be defensible from a public policy perspective even without the request (or even knowledge) of the user, and it can even be considered an application of a broader interpretation of the once-only principle; but the SDGR does not allow such exchanges in principle, subject to the exceptions discussed below. By way of a practical example: the technical system can be used under the SDGR to allow the user to provide evidence that they are eligible for a particular service or benefit at the time when they apply for it. The system however cannot be used to allow the competent authority to continue to obtain evidence afterwards whether these requirements are still met, unless the user chooses to cooperate.

There are some theories on how the concept of a 'request' could be interpreted to none the less accommodate such models. One might e.g. consider the case where a user explicitly requests that a certain administration obtains certain evidences for a specific procedure, and that it asks that it keeps these up to date (including through future requests) for a specified period of time. In this case too, the exchanges are arguably based on an explicit request, the scoping of which could be clearly approved by the user. While each subsequent exchange (resulting from the initial request) is not the result of an entirely new request, there is no part of the Regulation's phrasing that suggests that individual requests for individual exchanges would be necessary.

None the less, there are some constraints that impede an easy adoption of such models as a part under Article 14. Firstly, there is the consideration that the original request would at any rate need to be particularly clear and explicit on the scoping of the request, and in particular on the possibility of future exchanges, including purpose limitation and temporal limitation. A situation where a competent authority can request evidences without any limitation to specific administrative procedures or for an indeterminate period of time would not be compatible with the SDGR. Secondly, the Regulation also contains a preview requirement as will be examined below: the user must be able to preview each subsequent evidence exchange and be permitted to decide whether to proceed with it.

This latter element inherently requires user involvement, so that automated exchanges without user involvement are unlikely to comply with Article 14.

There are exceptions to the request requirement. As the Regulation notes, the "use of the technical system […] shall only be permitted at their explicit request, unless otherwise provided under Union or national law" (14.4 SDGR). This exception could be applied to evidences which are publicly available to anyone without any constraints (e.g. via public websites, open web services, etc.). In such cases, it seems reasonable to argue that automated cross-border exchange without a request is also allowed. Secondly, it could also be reasonably applied to evidences which are available to be exchanged between designated competent authorities within the EU (without constraint to one or several specific Member States). Company information that can be exchanged between business registers via the BRIS network seem to be an example, since the BRIS legislation allows competent authorities to exchange information directly in the circumstances covered by that legislation (without the request by the user). In such cases it seems reasonable to argue that automated cross-border exchange without request is allowed via the technical system as well.

It is worth noting that national or European law could also have the inverse impact: rather than just eliminating any need for an explicit request (and permitting exchanges even without users explicitly requesting it), it would also be possible for such laws to mandate use of the technical system – not only eliminating the requirement of a request, but even invalidating the possibility of choosing alternative means of submission of evidence. In other words, future evolutions in European or national law can significantly impact the scoping of the use of the technical system.

The Preview Requirement

According to the Single Digital Gateway Regulation, the envisaged technical system "*shall enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence*" (14.3 (f) SDGR). Recital 47 clarifies that the user can exercise that right not to proceed *"in cases where the user, after previewing the evidence to be exchanged, discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question."*

The technical system must thus support a mechanism of preview by the user of the evidence, and a mechanism of approval of the exchange after observing the preview (thus also preventing the exchange by refusing to approve it). However, the wording of the preview mechanism in the SDGR clearly indicates that the preview is only a *possibility* that must be afforded to the user, not that the user has to be required to actually use (observe) the preview.

The preview mechanism aims to support the accuracy and relevance of the data exchanged and strengthens control by the user over data exchanged through the technical system, allowing them to exercise some control over the consequences of their use of the system.

The English language version of the SDGR does not state explicitly when the preview should take place; it merely notes that the technical system should "enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence". Given this

phrasing, the most rational interpretation is that the preview possibility is offered to the user *before* the exchange of evidence to the receiving authority occurs. A broader interpretation, where the receiving authority first receives the evidence and then allows the user to preview it and to block any use of the data, arguably raises compliance challenges with the phrasing of the SDGR. Other language versions of the SDGR are more explicit than the English phrasing in requiring a preview before the exchange occurs. E.g. in German, the Regulation requires the technical system "*dem Nutzer die Möglichkeit bieten, die von der anfordernden zuständigen Behörde zu verwendenden Nachweise vorab einzusehen und zu entscheiden" – vorab* indicating that the preview occurs before the exchange.

From a functional perspective, the principal objective is at any rate that the evidence can only be used for a preview, and not for the actual procedure itself, until the evidence exchange has been approved during the preview (or until the user declines the possibility to preview).

Similar to the explicit request, the SDGR indicates that the possibility of a preview is not required when "automated cross-border data exchange without such preview is allowed under applicable Union or national law" (14.5 SDGR). Again, the exception could plausibly be applied to evidences which are publicly available to anyone without any constraints, and to evidences which are available to be exchanged between designated competent authorities within the EU.

One additional complexity is the issue of which 'national law' determines whether a preview can be omitted or not. The simplest interpretation is that the main relevant question is whether the evidence is publicly available without constraints – and therefore that only the national laws of the data providing Member State govern the preview exception. However, a much stricter interpretation could be applied as well, in which the omission of a preview is governed by any national laws determining the rules behind a specific procedure. In that interpretation, the national laws of the data consuming Member State are equally relevant – i.e. if an evidence is freely available in Member State A, but Member State B does not recognise the free availability of that type of evidences in a specific procedure, Member State B might insist on previews, arguing that its own laws are not complied with if no preview was available. This is an open issue at present.

Finally, recital (47) of the SDGR also indicates that "the data included in the preview should not be stored longer than is technically necessary". Given the reference to technical necessity, this constraint seems to target only the storage required for the preview functionality, and not any storage that precedes or follows the preview (e.g. retention in the sending Member State for accountability purposes, or retention in the receiving Member State for the purposes of administrative follow-up of the service requested by the user).

In addition, the reference to "data included in the preview" seems to suggest that it is principally the evidence's content that may not be retained longer than necessary, which is reasonable from a data protection and confidentiality perspective. No part of this provision would seem to suggest that an audit trial is impermissible, provided that the audit trail doesn't include the "data included in the preview". In other words, an audit trail could contain any metadata related to the preview process, as well as e.g. hashed

values of the evidence file in order to determine afterwards (in case of disputes) whether a specific file was exchanged, provided that the evidence itself and its contents are not retained.

Based on that understanding, the main implication seems to be that the technical system must include a function that ensures that an automated deletion of the evidence should occur after the user decides whether or not to transfer the evidence. This deletion (from static storage devices or from dynamic memory) should be verifiable through an appropriate log or audit trail. No centralised storage of the evidence is permissible under the SDGR.

Freedom to Choose

As a third pillar to the SDGR's user centricity (in addition to the user request and the preview requirement), Recital 47 of the SDGR indicates that the use of the technical system should be voluntary, and that other means of submitting evidence should remain available to users. This principle is repeated in Article 14.4, which notes that "*The use of the technical system shall not be obligatory for users and shall only be permitted at their explicit request, unless otherwise provided under Union or national law. The users shall be permitted to submit evidence by means other than the technical system and directly to the requesting competent authority*".

In other words, users can never be forced to use the technical system. This does not imply that the use of electronic communications cannot be made compulsory under national law; this is a matter of national sovereignty. However, if users do not wish to use the technical system, they must be provided with alternatives, which may be digital or analogue, as deemed permissible by the national laws governing the procedure.

2.4 Data Protection as a General Consideration Behind the SDGR

Applicability of Data Protection Law

A general concern in relation to the once-only principle is compliance with the EU's fundamental right to data protection, as enshrined in article 8 of the EU Charter of Fundamental Rights, and as governed principally by the General Data Protection Regulation. While not all evidences exchanged via the technical system will by definition qualified as personal data, it is clear that most evidences will contain at least some personal data, and that the requirement of human involvement (through the user) in any evidence exchange implies that at least some personal data processing is required for any application of the once-only principle as envisaged under Article 14. After all, the user will be identified, and information about the time, source and destination of the exchange will need to be generated and logged, as well as the nature of the evidence. Collectively, this already entails a processing of personal data.

Legal Basis for the Processing of Personal Data

The explicit request requirement to some extent helps to support compliance with key data protection principles under EU law, in particular the requirement to have a legal basis for a transfer of evidences containing personal data. The SDGR comments on this relationship explicitly, noting that "Where the exchange of evidence includes personal data, the request should be considered to be explicit if it contains a freely given, specific,

informed and unambiguous indication of the individual's wish to have the relevant personal data exchanged, either by statement or by affirmative action. If the user is not the person concerned by the data, the online procedure should not affect his or her rights under Regulation (EU) 2016/679".

This assertion is short, but contains a few critical pointers for the interpretation of the relationship between request and consent. Notably, it recognises that not all evidences will include personal data. This is of course dependent on the procedure and on the evidences required. Furthermore, the recital's meaning should not be misunderstood as saying that a request under the SDGR is identical to consent under the GDPR. It notes only that, if evidences contain personal data and a consent meeting the requirement of the GDPR is obtained for the exchange, then the consent requirement also satisfies the requirement of the explicit request. It however does not indicate that a consent meeting the requirements of the GDPR is always required, nor that every request under the SDGR satisfies the requirements of a consent under the GDPR.

To understand the exact relationship between the request and a consent, it is important to understand that any exchange (or other form of processing) of personal data through the technical system must comply with the requirements of the GDPR. A central challenge in any SDGR procedure – among other data protection challenges – is ensuring that there is a legal basis for the transfer of evidence, assuming that the evidence indeed contains personal data. It would be tempting to assume that the explicit request of the user to transfer any personal data constitutes a consent under the GDPR, and therefore that it is sufficient as a legal basis in all cases. None the less, this would be incorrect for several reasons.

Firstly, a consent under the GDPR must be given by the data subject, i.e. the person whose data will be processed. This is sometimes not possible in specific procedures, where the user may not be the (only) person whose personal data will be processed – consider e.g. an accounting person using the SDG to transfer personal data relating to the management of a company: the accounting person cannot by definition provide consent on behalf of the management.

Secondly, consent under the GDPR must be freely given. It has been a long standing interpretation of European data protection law – and this point has been recently affirmed in official guidance from European data protection authorities – that freely given consent is not possible when there is a clear imbalance of power between the data controller (the party asking for the consent) and the data subject (the party giving their consent). The aforementioned Guidelines take a very strict approach on this point, and stress that "it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities". While this position appears strict, it is not illogical: in the case of e.g. moving one's home to a different Member State, there is hardly any freedom left: a citizen either consents, or is unable to move homes. In these circumstances, there is little choice in reality, and therefore no way to provide a consent satisfying the requirements of the GDPR.

Similarly and perhaps less intuitively, the same Guidelines note that "an imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee".

In both cases – public authorities and employees – consent is not entirely impossible if there is indeed no imbalance of power, but it is generally not the favoured legal basis for the processing of personal data under European data protection law. However, this is not an insurmountable problem in practice, since the GDPR does not require consent by definition, but rather a legal basis, for which consent is only one available option. The SDGR similarly does not mention consent at all – nor any other legal basis under the GDPR – thus leaving multiple justifications open. As the European Data Protection Supervisor also noted in its Opinion 8/2017 on the proposal for the SDGR, "the three most relevant legal grounds for implementing the 'once-only' principle are consent, legal obligation and public task/official authority. Depending on the circumstances, one or another of these legal bases could be the most appropriate choice. As a general rule of thumb, for the case of any recurring and structural data sharing, the EDPS recommends - in order to ensure legal certainty- that whenever possible, further processing of personal data based on the once-only principle be specified in a legislative instrument, which provide appropriate safeguards to ensure compliance with data protection law, including the principle of purpose limitation and ensuring data subjects' rights".

Thus, it is clear that consent in the sense of the GDPR is not a requirement for the exchange of evidence, and that the procedural prerequisite of the SDGR of an explicit request should not be conflated with a GDPR consent requirement: the explicit request obligation may apply even in cases where there is no personal data involved, and inversely a legal basis for the exchange of evidence must exist even when there is an exception to the explicit request requirement. The two obligations – explicit request and legal basis – exist side by side, and are separate.

In some procedures, the choice for a GDPR consent as a legal basis for the exchange of evidence is plausible, but in many (including those where consent is not possible) a different legal basis will need to be relied upon. While the choice can be different from use case to use case, the legal basis will generally be the legal obligation for the competent authorities to transfer evidences under EU or national law; or the legal obligation for the competent authorities to transfer evidences as a part of the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. To the extent that the SDGR creates the obligation for competent authorities to cooperate in such exchanges, an appropriate legal basis under the GDPR is thus available.

Once-only and Further Processing of Personal Data

The once-only principle relies essentially on the reuse of data previously created, collected or stored by public administrations in relation to citizens and businesses; indeed, such reuse is even its sole purpose. Where the information exchanged through the application of the once-only principle includes personal data, issues concerning 'further processing' as described under the GDPR must be addressed. The notion of further processing, which is processing of personal data beyond the initial purpose for which it was collected, is tied to the principle of purpose limitation.

Under the GDPR, purpose limitation is a fundamental data protection principle according to which data is collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes (Article 5.1 GDPR). There are exceptions, when the data subjects consented to the further processing or when or when it constitutes a necessary and proportionate measure in a democratic society to safeguards certain of its fundamental elements (such as listed in article 23 of the GDPR). As highlighted by the European Data Protection Board, easing administrative burdens on individuals or organisations is one of the primary aims of the once-only principle, and is undoubtedly of public interest. None the less, processing of personal data for other purposes should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected (Recital (25) GDPR).

The compatibility of purposes must be assessed based on the link between the new purposes, the context of the processing, the nature of the data concerned, the possible consequences of the processing and the existence of appropriate safeguards (Article 6.4 GDPR). In the case of further processing through the technical system set up in compliance with the SDGR, the compatibility of purposes is largely governed by the legislator at EU level: the existence of the SDGR and its explicit requirement to apply the once-only principle in the listed procedures, under the safeguards stated in the SDGR, fundamentally implies that the further processing required by the SDGR is considered as compatible with the original purposes by the legislator. Of course, compliance with the safeguards of the SDGR is critical in this assessment, and notably the obligation in principle to only use the technical system at the explicit request of the user, or when required under Union or national legislation.

On this basis, the further processing of personal data under the SDGR must prima facie be deemed as compatible with the original purposes.

For the avoidance of doubt, it is clear that the SDGR also contains a purpose limitation principle, which notes explicitly that "The evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used by that authority for the purpose of the procedure for which the evidence was exchanged" (Article 14.8). However, it would appear logical that use of the evidence "for the purpose of the procedure" must include any use that's mandatory under national law as a result of that procedure. Otherwise, use of the SDGR would make it impossible for receiving competent authorities to respect national laws, such as archiving laws, since these too are essentially a form of further processing.

3 Challenges and Ambiguities

3.1 Reliance on Further Implementation

The analysis above has already shown that there are some ambiguities still on the exact interpretation of the SDGR, and the way the technical system will need to be implemented centrally and at the Member State level. Many of these are expected to be resolved through the adoption of one or more implementing acts by the European Commission, which should be in place by 12 June 2021, as required by Article 14.9 of the SDGR. These acts should set out the technical and operational specifications of the technical system.

In the sections below, we will briefly examine some further points of contention, which will likely be at least partially mitigated by the implementing acts.

3.2 Requirements for the User

As has been noted in the introduction above, the Regulation's approach is user centric in principle, since exchanges of evidence must be triggered by an explicit request from the user (subject to certain exceptions). Users can be either natural persons or businesses, since users are defined explicitly in the Regulation as "either a citizen of the Union, a natural person residing in a Member State or a legal person having its registered office in a Member State, and who accesses the information, the procedures, or the assistance or problem-solving services, referred to in Article 2(2), through the gateway".

The scoping is thus relatively broad, and it is worth noting that citizenhood (to be understood as having the nationality of a Member State) is not a prerequisite for eligibility to use the technical system. For a natural person, it is sufficient to have a residence in a Member State. Legal persons on similarly are required to have at least a registered office in a Member State.

While this approach is succinct and pragmatic, it also hides a significant degree of complexities that still need to be resolved, both technically and legally. The complexity stems from the fact that the Regulation envisages that the covered procedures can be completed in a fully online manner (Article 6), meaning that:

(a) *the identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way;*
(b) *users are provided with an automatic acknowledgement of receipt, unless the output of the procedure is delivered immediately;*
(c) *the output of the procedure is delivered electronically, or where necessary to comply with applicable Union or national law, delivered by physical means; and*
(d) *users are provided with an electronic notification of completion of the procedure.*

Thus, an important legal prerequisite is that users – natural and legal persons – can be identified electronically, that they can obtain the relevant evidence electronically, and that they can submit it electronically. This is not a trivial issue in practice. An important pre-existing input on this topic is the existence of the eIDAS Regulation(EU) No 910/2014,

which regulates the recognition of national means of electronic identification by public authorities in cross border transactions, and also provides a legal framework for electronic signatures and electronic seals that may be used to authenticate evidences. However, there are several challenges on this point.

Firstly, the Single Digital Gateway Regulation does not contain a requirement to use means of electronic identification which are subject to the terms of the eIDAS Regulation. Recital (70) does note that "Member States are encouraged to increase the security of transactions and to ensure a sufficient level of confidence in electronic means by using the eIDAS framework laid down by Regulation (EU) No 910/2014 and in particular adequate assurance levels. Member States can take measures in accordance with Union law to safeguard cybersecurity and to prevent identity fraud or other forms of fraud". However, this is merely an encouragement, not an obligation.

While use of electronic identities that are recognised under the eIDAS Regulation – meaning that Member States have completed a notification procedure for these identities – is a partial solution, it does not resolve all challenges. At the time of writing, 14 Member States have a notified eID scheme – which is a substantial but not universal coverage. Furthermore, completing the notification process hardly resolves all legal challenges. The eIDAS Regulation recognises three tiers of quality of eID schemes (referred to as levels of assurance): low, substantial or high. There is no consensus at this stage which level of assurance should be adequate to permit identification within the technical system. While virtually all notified eID schemes achieve a 'high' level of assurance (meaning that they should open all relevant doors), there are some exceptions.

Secondly, even if all Member States would have a notified eID at the high level of assurance, that would still not comprehensively resolve all challenges for identifying users. Specifically for legal persons (i.e. companies or organisations represented by a specific natural person), there is no unambiguous legal framework yet for establishing the right of the natural person in any given procedure to represent the legal person in a given procedure. In simpler terms: neither the legislation nor the available infrastructure is currently capable of creating complete legal certainty on whether a specific person trying to access a procedure on behalf of a company is legally permitted to represent that company, or to obtain evidence for that company, or to submit it on that company's behalf. While pilot level solutions exist for this problem, the legal framework (and notably the eIDAS Regulation) has not yet been revised to create certainty on this point.

Thirdly, in order to resolve this problem, one should also take into account the potential multitude and variety of participants in an evidence exchange under the Single Digital Gateway Regulation. Insofar as a user interacts with a public authority targeted by the eIDAS Regulation, acceptance of a notified means of identification should be legally certain. However, evidences may be obtained from entities that do not normally interact with citizens in e-government procedures, or that may not unambiguously qualify as public authorities who would be obliged to accept notified electronic means of identification under the eIDAS Regulation (e.g. universities, who may need to provide electronic diploma's as a part of an Article 14 procedure). Therefore, even the universal applicability of the eIDAS Regulation would not comprehensively solve the identification and authentication challenge: the evidence providers may not currently support notified

means of electronic identification, and moreover their own approach to user identification may not be technically capable of linking users unambiguously to an eIDAS notified eID.

Ultimately, this is largely a question of the extent to which competent authorities are willing to trust each other's procedures for the identification of users. If this trust is low, then a strict application of the eIDAS Regulation may be advisable, e.g. by requiring that evidences must be retrieved based on identification procedures using a high level of assurance under the eIDAS Regulation, and that proof of the use of such means of identification is presented. If trust is high, then other means of electronic identification could be permitted as well. Choices on this point, which are partially political and partially driven by objective risk assessment, will need to be made by the implementing acts.

3.3 Requirements for Competent Authorities

As noted in the introduction, a principal difference between national level once-only legislation and the SDGR is that national legislation can directly target specifically identified competent authorities, for the simple reason that they are known or at least identifiable under national law. The same is not true at the EU level, where administrations can differ widely from Member State to Member State, in terms of their designation, competences and capabilities.

For that reason, the SDGR applies a very open model, which focuses on high level identification of covered procedures, and succinctly notes that competent authorities comprise "any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation" (Article 3 (4)).

In other words, the relevant authorities are those entities which are tasked with specific responsibilities in relation to the covered procedures. In practical terms, this approach leaves Member States the greatest possible flexibility (and corresponding responsibility) in identifying entities which are affected by the SDGR. The consequence of this approach is also that a 'competent authority' is not necessarily a traditional public sector body. If a private sector entity is a body charged with these tasks, it will be qualified as a competent authority under the SDGR as well, and Member States will need to take measures to ensure that such entities can also provide evidences or accept them in the covered procedures.

Finally, it is worth underlining that the SDGR's provisions on the once-only principle as such do not require digitization of evidences and the underlying procedures. Article 14.2 notes that "where competent authorities lawfully issue, in their own Member State and in an electronic format that allows automated exchange, evidence that is relevant for the online procedures referred to in paragraph 1, they shall also make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange".

The phrasing ("where" they issue) indicates that the clause is conditional: the authorities must also make evidence available in the context of the SDGR where it is already issued – if it is not issued in such a format, or if the issued evidence is not relevant to the online procedures, then there is no obligation for a Member State to move to such a

format. More simply put: Article 14 does not create a legal obligation to issue electronic evidence at.

For completeness sake however, it should be recognized that Article 6 of the SDGR does contain an obligation for Member States to ensure that some procedures are offered fully online, which may result in evidences becoming available in an electronic format if the procedures require evidences; but the SDGR does not contain a direct legal obligation for Member States to introduce new types of evidences, or to provide electronic versions of them.

3.4 Requirements for Evidence

As noted above, the only evidences that must be made available for exchange within the scope of the SDGR are those which are already issued "in an electronic format that allows automated exchange". If such evidences are available, they must also be made available in the same format.

This raises a key issue: when exactly can evidence be considered to be "in an electronic format that allows automated exchange"? More specifically, does this description imply that the evidence must be formatted in a semantically meaningful way – i.e. must it be structured in a way that allows the evidence to also be interpreted and processed automatically, at least to some extent, by the receiving competent authority? Or from the opposite perspective: does it imply that unstructured evidence, such as a graphic image (a bitmap, JPEG, or PDF scan without a semantic structure), should not be considered to be evidence falling within the scope of Article 14?

The concept of evidence "in an electronic format that allows automated exchange" can be interpreted and scoped in many ways. Generally speaking, "evidence" is a fluid concept, that should not be simply equated to standardised formal documents, comparable to the traditional way of working in an analogue environment (e.g. through standardised birth certificates, statements of domicile, extracts from criminal registers, etc.). In a digital environment, a much more granular approach is possible.

Increasingly, evidences are no longer supplied as static documents. Rather, evidences are nowadays often available as the result of a dynamic process, consisting of a concrete response – sometimes as simple as a yes/no assertion – to a specific question. For instance, to prove that someone has permission to drive a certain type of car, it is not necessary to transfer comprehensive driver's license records. It suffices to query a register whether a specific person is allowed to drive. If the register only answers „yes" or „no", the 'evidence' is a minimal but perfectly suitable assertion, that would optimally preserve privacy.

There is still some discussion at present to what extent fully unstructured electronic evidences would satisfy the requirements of the SDGR. Based on the lack of constraints on this point in the SGDR, it seems that evidence requesting competent authorities cannot reject evidence in an unstructured format. It is the issuing Member State that determines which evidence is lawfully issued and how, in accordance with its own national laws. There is no legal basis for a receiving Member State (or a receiving competent authority) to reject evidence because it does not meet its formatting/structure expectations. For completeness, it can be noted that a receiving Member State may require additional documentation to be provided, such as translations of the evidence.

Since this means that semantic information may be missing from the evidence, it is all the more important for the technical system to ensure that at least sufficient metadata or some other form of semantic context is included during the exchange, to allow the receiving competent authority to interpret the nature and content of the evidence. As a result, the technical system should be designed in a way that allows this metadata or semantic context to be discovered during an evidence exchange, either because the metadata or semantic context is embedded in the evidence itself (which would be the optimal scenario), or because the exchange is accompanied by metadata that contains the relevant semantic context and corresponding information in the evidence.

There is one further layer of complexity relating to evidence in the SDGR. Article 14.8 requires that evidences must be "limited to what has been requested", which raises some concerns on the common practice of providing standardized evidentiary documents that contain substantially more information than required. By way of example, if a competent authority wishes to receive evidence of the date and location of birth, it may receive a birth certificate that contains not only those data points, but also information which is not strictly needed (e.g. identity of the attesting doctor or public official, identity numbers, identity of the parents, etc.). This is of course suboptimal from a data protection perspective, since more data is exposed than would be strictly necessary.

None the less, if such documents are the available and relevant evidences in the issuing country, it seems that they satisfy the requirements of the SDGR, even though they are arguably a practice that's subject to significant improvement.

3.5 Requirements for Data Flows

As an application of the once-only principle, Article 14 requires that the technical system allows the automated exchange of evidence between competent authorities in different Member States – a flow which therefore goes from administration to administration. Similarly, it notes that the authorities must "make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange". These provisions strongly suggest a direct exchange, where evidence is requested by one competent authority from another, and provided by that competent authority in response.

None the less, as the sections above in relation to request and preview have illustrated, the reality is not so straightforward: while one competent authority may request evidence from another, that request must in principle be preceded by a request from the user. It is presently still an open question whether the evidence issuing authority may insist on proof of the original request from the user, or whether it is simply required to trust that the requesting competent authority has met all applicable requirements. This issue too will presumably be addressed in the implementing acts.

Similarly, the preview requirement indicates that evidence does not simply flow from one competent authority to another upon request: it must be made available for preview to the user, which implies that it is transferred first to the user (possibly merely as a visual representation rather than as a comprehensive file). Since the communication to the user for the purposes of a preview will typically be needed, it also seems defensible that the evidence is not transferred directly from one authority to another, but rather that it passes through the user, e.g. via a controlled end user environment. This approach can

be in line with the once-only principle, provided that it is organized in a clear data flow that allows the user to continue his or her administrative procedure seamlessly – in other words, provided that the implementation does not simply result in the user receiving their evidence and then being left to their own devices.

In ideal circumstances, relevant evidence will be immediately available upon request. However, there are situations where evidence will need to be collected or created upon request, e.g. because the relevant evidence is only available on paper and requires digitization. This implies an interrupted procedure, where a user initiates a procedure and evidence is requested, but the procedures is thereafter halted temporarily – potentially for hours or days – while electronic evidence is created. This is a challenge for the vision of the SDGR, due to the preview requirement – evidence that does not yet exist cannot be previewed, meaning that the session will need to be interrupted. This is not legally problematic under the SDGR, since it contains no requirement that evidences must be available instantaneously or that procedures must be completed immediately. However, from an infrastructural perspective it does create problems: since users cannot remain logged into a session for days, such interrupted procedures imply the creation of some form of personal information management system where procedures can be put on hold until all information requirements are met.

As a final challenge in implementing smooth data flows, there is also the problem that some evidence may not be available for free. In SDGR procedures, it is possible that a user has to pay to obtain certain evidences from an issuing authority. By way of examples, an extract from a business register may not be free, or even a birth certificate could in theory require a charge covering the administrative cost born by the authority.

The SDGR does not affect this ability to charge. It contains a section requiring Member States to ensure that electronic payments are possible for the completion of online procedures, namely Article 13.2 (e), which notes that "where the completion of a procedure requires a payment, users are able to pay any fees online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union". However, this provision clearly is applicable to the payment by the user of a fee to the competent authority requesting evidences for the cost of the administrative process. It does not address the payment of a fee to the competent authority providing evidences (the data provider).

It appears that the SDGR is silent on the issue of payment to evidence providers, and therefore that there is no formal legal obligation for Member States or their authorities to modify or eliminate their charging policies in the context of the SDGR. In other words, if the issuing competent authority already charges a fee to the user for evidences outside of the context of the SDGR, they can also do so for procedures covered by the SDGR.

4 Concluding Notes and a Perspective on the Future

4.1 The SDGR as a First Step into a European Once-Only Framework

As this contribution hopes to illustrate, the SDGR is a milestone achievement for European e-government. It is the first attempt to create a legal framework for cross-border once-only functionality, and successfully defuses many of the inevitable challenges that

arise at this scope, such as the need for user control (through the request and preview requirement), the difficulty of identifying competent authorities and relevant evidences (by focusing on enumerated procedures rather than on the entities and documentation behind them), and the freedom of the user to elect *not* to use the system if that is their preference.

None the less, the SDGR is not without its challenges. Its closed list of procedures means that it has limited flexibility to grow without further regulatory intervention. Its insistence on user control ensures that the once-only principle cannot be applied to enable verifications or recurring exchanges without user approval, even when this would be manifestly in the public interest. And there are very many topics – user authentication needs, semantic structure of evidence, interrupted procedures, the right for competent authorities to check each other's work, and payment for evidences, to name but a few – which are left open to further implementation and interpretation.

As such, the SDGR is truly the first step in this evolution: it is ambitious and challenging in its own right, but unlikely to be the conclusion of the once-only model.

4.2 Once-Only as an Evolving Story of Trust

To at least some extent, the constraints built into the SDGR are merely indicative of the current technical state of play, and of the need for Member States to establish a first measure of experience in direct evidence exchanges before engaging in even more ambitious variations on this theme. Even if the implementation of the SDGR as envisaged in Article 14 is fully successful, revisions of the functional model and the legal framework are inevitable.

Beyond extensions of the number of procedures to be covered, it is likely that at least some Member States will want to examine the possibility of direct exchanges of certain data *without* a prior request from the user – as is already permitted under many national once-only laws – including through data subscription models where any changes in the data are automatically communicated. Inversely, some Member States will want to work in an even more user centric manner, where citizens and companies have their own decentralized but protected personal data spaces, in which they can store and reuse evidences as they please, including by providing them to any desired recipients, rather than just those enumerated under European once-only law.

These approaches are neither inevitable, and nor are they necessarily superior to those of the SDGR. Rather, they are indicative of a different trust model, and of an evolving perspective on an ideal e-government or even on an ideal information society. Future trends are hard to predict, but in all likelihood, the SDGR will not prove to be the end station for European once-only legislation.

References

1. Author, F.: Article title. J. **2**(5), 99–110 (2016)
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016)
3. Author, F., Author, S., Author, T.: Book title, 2nd edn. Publisher, Location (1999)

4. Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)
5. LNCS Homepage. http://www.springer.com/lncs, Accessed 21 Nov 2016