Summary

More than 150,000 people pass away each year and about the same number of estates are settled. Almost without exception, the deceased leave behind digital 'assets' such as social media accounts, e-mails, documents stored in the cloud and (user rights to) all kinds of media and entertainment. The question is whether the current Dutch legal framework offers sufficient levers to safeguard the private and public interests involved in the settlement of digital estates. The central research question of this study is: *what adjustments to the Dutch legal framework, if any, are desirable to adequately protect private and public interests involved in the settlement and liquidation of digital estates?*

To answer this question, first an analysis was made of relevant terms & conditions that providers of commonly used information services apply, and of their policies regarding death. The analysis included user agreements, general terms and conditions, privacy policies and other available company documents. Information service providers were categorized into digital media services (commercial offerings such as streaming video or music), communication services (including social media and messaging services) and ICT services (including cloud storage and digital safes). Next, the relevant legal framework is described, and ambiguities therein are identified. In addition to inheritance law, this concerns contract law and, in particular, consumer law, intellectual property rights (especially copyright), personality rights and data protection law (General Data Protection Regulation). General property law is also important, insofar as it relates to the question whether digital assets are part of the estate. Finally, with a view to formulating possible solutions, a selection of legislation in other countries was studied.

The general picture that emerges from the **analysis of the terms & conditions** is that, to date, information service providers pay little explicit attention to the handling of digital content in the event of the death of users. An important conclusion is that it is difficult for users to get a grip on what happens to accounts and the associated digital content in the event of their death. This is due to the lack of a clear policy on the part of service providers, a complex legal framework and due to the great diversity of conditions. This diversity is partly a logical consequence of the variety of services and the freedom of contract. The (legal) uncertainty exists for the user who wants a say in what happens to data after death, but also for the next of kin, or to be more precise: heirs and possibly authorised representatives.

Some large providers (such as social media platforms Facebook and Google) do have clear(er) policies and related facilities. This is also true for providers of digital safes. They have different forms of a 'trusted persons policy', whereby people specifically designated by the deceased user can gain access to (part of) the digital content, or can, for example, put accounts in a 'memorial mode'. Other forms of policy and conditions concern the retrieval of account data and content by heirs or other third parties; the takeover of the account by heirs or other third parties; and the possibility for heirs or other third parties to terminate an account.

An **analysis** of the **applicable legal framework** mainly shows that legal uncertainty still exists in many areas. This uncertainty does not stem so much from inheritance law itself, but from a lack of clarity as to what digital assets are part of the estate at all, such as data, the content of accounts (apart from intellectual property rights), virtual 'objects' and portrait rights on images of people. These are therefore questions of (general) property law. Current contract law, and especially consumer law, is not geared to the specific problems of the legal status of digital content left behind after death, such as account information, user-generated content, materials stored with cloud storage services and purchased media. Can this content, for example, 'disappear' from the view of heirs through 'no survivorship' clauses, which stipulate that upon death the user agreement ends, or are such clauses unreasonably onerous?

When it comes to intellectual property rights, and especially copyright, an underexposed problem is that users themselves are increasingly the copyright holders because they create and post content that

qualifies for protection. This is especially true for communication services (principally social media and chat apps). Since copyrights are part of the estate, the question arises as to what the shift to the cloud means for the actual control that the testator and heirs have over these property rights. Contemporary thought on these kinds of questions is not yet very developed.

A third legal domain relevant to data protection after death concerns privacy and data protection law. There is no clear recognition in Dutch law of any general right of personality that would have effect after death; the same applies to a right to protection of the privacy of the deceased. Also, the General Data Protection Regulation (GDPR) is currently not applicable to the personal data of deceased persons; the Dutch legislator deliberately chose not to extend the GDPR. However, there are various rights and obligations in data protection law that offer a starting point for dealing with the interests of users of information services in the event of death.

Little is known about the societal norms around data after death, about people's expectations concerning the existence of post-mortem privacy, and how these expectations may be changing as our lives become ever more digital. Flash surveys previously commissioned by government shows that the majority of Dutch people are not familiar with the concept of 'digital estate' and do not make arrangements regarding what happens to their data after death. It seems advisable to gain a better picture of social opinions by means of (empirical) research. These are relevant to the social acceptability of virtually any policy intervention in the field of digital legacies. This is particularly the case when it comes to the question of the desirability of granting next of kin (family, partners) and heirs (not necessarily immediate family) access to all or certain digital communications of the deceased, and who should or can regulate, in what way, what happens to digital property after death. Of particular importance here is what facilities are expected from service providers, and what the legal status is of choices made by users after death (e.g., with respect to designating an authorized person to have access, or choices to have data deleted after death).

Based on the analysis of the conditions used by service providers, the legal framework and the gaps identified in it, **solutions were** formulated **along three lines**. How other countries deal with the issue of digital legacy was also considered. The principles of legal certainty and autonomy are leading in all lines. Both principles play an important role in inheritance law, (consumer) contract law, personal data law and intellectual property law. Two of the three solution directions connect to existing domains, namely contract law (in particular consumer contracts) and data protection law. The third solution involves a specific legal regulation for dealing with digital property, following the example of 'digital assets acts' in the US and Australia, among others.

Within (consumer) **contract law**, several matters can be regulated that limit legal uncertainty for heirs and respect the autonomy of the user. Treating so-called 'no survivorship' clauses as unreasonably onerous places the burden on the service provider to demonstrate that there is indeed an interest in the lapse of the contract upon the death of the user, and in the deletion (or in fact the continued use by the service provider) of the digital content attached to it. Certainly, in the case of communication services (social media, messaging apps) and ICT services (email, cloud storage), the use of no-survivorship clauses is far-reaching: if the contract ends upon the death of the user, there will be no more access to the content of an account. Within consumer law, a (limited) right to portability could possibly be recognised, whereby certain content may be moved from the user's account to another account or device, with a view to ensuring access by heirs.

A more far-reaching contract law option is to strengthen the rights of users by giving them more direct control. Service providers would then be obliged, for example, to make provisions allowing users to determine what should happen to the data linked to the account in the event of death. Especially if large service providers who offer bundled services are obliged to do so, this will promote the autonomy of users. They will then have more control over much of their digital property at the same time (in social media accounts, cloud storage, email accounts, etc.), which is, after all, due to bundling and the creation of 'walled

gardens' often largely held by a particular provider such as Google, Amazon, and Apple. However, it should be further investigated whether contract law is the right domain for such a solution or whether a stand-alone digital legacy regulation would be preferable.

Another aspect where further regulation seems appropriate is to ensure that the contractual confidentiality obligations in relation to secure accounts do not extend to the sharing of data during lifetime with a view to providing access after death (to heirs in particular). Furthermore, access for heirs can also be facilitated by setting limitations on the burden of proof that service providers may impose on heirs. For instance, by stipulating that a (European) certificate of succession is sufficient, so that service providers cannot, as is currently the case, demand that the heir produce a court ruling.

A second solution lies in the area of **data protection law.** Certain rights and obligations from the General Data Protection Regulation (GDPR) could be continued post-mortem. For example, the so-called 'on hold provision' of Art. 18 GDPR can be declared applicable upon death, which would mean that personal data must be retained after death (e.g., for a period of 5 years), enjoy protection under the GDPR and may only be processed for specified purposes. Another option is to grant a right of deletion and possibly rectification of data to the heirs, the executor or trustee appointed by the deceased. In that case, the digital assets can be settled without giving access to all the personal data of the deceased. This can be particularly important when the privacy and other interests of third parties are at stake, such as with social media accounts and e-mail.

In exceptional situations, it could then be considered to grant other GDPR rights to the heirs, such as the right of access to all (personal) data stored about the deceased, if they have a clear interest in doing so. Here too, the interests of third parties, in particular the communication partners of the deceased, must be carefully considered.

Another basis on which access can be granted to heirs, for example, is consent or the execution of an agreement. Both grounds offer, in principle, room to let the person (data subject) determine which post-mortem processing is allowed - including giving access to e.g., heirs - by contractually recording it in such a way that the provisions continue to have effect. It is important to note that consent is only valid if it can also be unconditionally withdrawn (which, in the event of death, heirs would have to be able to do). The GDPR imposes strict requirements for consent to be valid.

With regard to preventing data from being orphaned or deleted after death, the GDPR's security obligation can be extended. In practice, service providers will often protect the remaining data of deceased users in the same way they do for living persons. However, if this protection is to be legally enforceable, it must be regulated, as, for example, the Irish legislator has done. The service provider must protect the data of deceased persons as if they belonged to a living person. A specific term can be set for this.

One aspect that deserves attention is enforcement. It makes a difference how a certain obligation is characterised. A (contractual) obligation may continue to exist after the termination of the agreement or consent; the associated claim to fulfilment then rests with the heirs. But the protection may also be one on which heirs or, for example, 'trusted persons' to be appointed may rely independently. It is also conceivable that an obligation of the service provider (data controller) can only be enforced by the supervisory authority, the Data Protection Authority (Autoriteit Persoonsgegevens) (e.g., post-mortem security). Incidentally, residents of the Netherlands already benefit from the *post-mortem* security obligation that applies in Ireland, since large platforms such as Google and Facebook offer services in the Netherlands from their Irish branches.

Finding a solution in the direction of extending the scope of the GDPR has more impact on some services and some parts of the digital estate than on others. After all, it will be required that personal data relating to the deceased are involved. The digital content (and tracking data) of a free communication service or a cloud storage service will generally consist of more personal data than, for example, the content of a subscription-based digital media service (although in those cases the service provider itself may collect a lot

of data on the user). However broad the GDPR may be, post-mortem application of certain rights and obligations from it would not cover all digital assets.

The third and last line is the creation of an **independent legal regulation**, a 'digital records act', inspired by existing initiatives such as those in the United States and New South Wales (Australia). This could take the form of a graduated system, whereby citizens can designate one or more authorised persons who should be able to access data from service providers after their death. Contractual conditions, e.g., regarding the secrecy of the login credentials of the deceased, cannot be invoked against them. However, such an arrangement could have far-reaching consequences, certainly when heirs are then by default granted full access to the digital assets if the deceased has made no provision for this. The social acceptability of this is uncertain; it would be advisable to investigate empirically the public's views on the desirable way of dealing with the data of deceased persons.

In the generic model, both the autonomy of the testator and legal certainty for those involved can be ensured, whereby in the choice of the specific design, one interest can be given more weight than the other. In the U.S., there is more room for the primacy of preferences laid down in tools, which is low-threshold and easy to change, but also offers less legal certainty. In Australia, on the other hand, an arrangement laid down in a will takes precedence over a subsequent designation of an authorised person via a service provider's facility (tool). Such a system would be more in line with Dutch inheritance law, and with the development of (notarial) services around digital inheritances that is emerging.

As noted above, without first gaining a good understanding of societal attitudes regarding post-mortem privacy and access by next of kin, the choice of a particular arrangement cannot be made properly. Seen from the perspective of EU law, there is **sufficient room for the Dutch legislator** to act on each of the three lines. Changes in consumer law should, however, be brought in line with the existing EU framework. For that matter, in view of the rapid development of European consumer law and the regulation of information services, it is advisable to aim for new regulations at the EU level. In the European context, it is also obvious to seek alignment with the GDPR now that the possibility is being offered to declare it (partly) applicable to personal data of deceased persons and this instrument is already being used elsewhere in Europe. An independent Dutch regulation based on, for example, the Australian digital assets act model has the advantage that the legislator is not dependent on the existing conceptual framework of the GDPR or (consumer) contract law, and that autonomy and legal certainty can be put first. If a choice is made for a Digital Records Act, it is recommended to opt for a minimal scenario, whereby the heirs are only granted access to data that are strictly necessary for the settlement of the estate, and only if the deceased has not stipulated otherwise. When a clearer picture is obtained of society's views on this, a more far-reaching standard scenario can be chosen.

Political feasibility naturally also plays an important role in the choice of a solution direction. Finally, it is important to note that, in addition to adapting the regulatory framework, systematic education about aspects of digital inheritance and awareness campaigns also seem indispensable to make it clear to citizens what is possible and permissible with their 'digital assets' after their death, and how they can make arrangements for dealing with them during their lifetime. Privacy research has shown that the ability of the average citizen or consumer to make conscious choices is limited if those choices must be made frequently and based on a lot of information (for example, accepting cookies on websites and user conditions of apps). People's concerns about privacy and data security do not immediately translate into concrete mitigating behaviours. This so-called privacy paradox is important to keep in mind when designing legal regimes for digital inheritance.