8

Public Registers Caught between Open Government and Data Protection – Personal Data, Principles of Proportionality and the Public Interest

GEERT LOKHORST[1] AND MIREILLE VAN EECHOUD[2]

Abstract

For governments across the globe, public registers are an increasingly popular means to help achieve a range of objectives. These include safeguarding the independence of judiciary, upholding food hygiene and safety standards, fostering proper use of subsidies, and protecting the public from unqualified professionals. Most public registers are subject to data protection laws because they contain some form of personal data. In the Netherlands, the number of online public register has risen dramatically. On the basis of exploratory research on Dutch public registers, we hypothesised that governments easily assume that public registers serve their designated goals, but rarely adequately assess their effectiveness. A comprehensive analysis of registers confirms that hypothesis is correct. This is problematic from the perspective of the EU's General Data Protection Regulation (GDPR) and the human right to privacy as enshrined in, for example, Article 8 of the European Convention of Human Rights (ECHR). Both require that the means used to serve a (legitimate) purpose are proportionate to the (potential) privacy harms. Based on the experience in the Netherlands, in this chapter we query to what extent and by which means policy and lawmakers actually test effectiveness of public registers and analyse the privacy implications from the perspective of proportionality. The adoption of open government policies combined with technological possibilities result in a strong growth of online public registers, and possibilities to link data from multiple sources multiply. The potential privacy impacts on individuals need to be better understood and safeguarded already at the design stages of public registers.

[1] Institute for Information Law, University of Amsterdam.
[2] Institute for Information Law, University of Amsterdam.

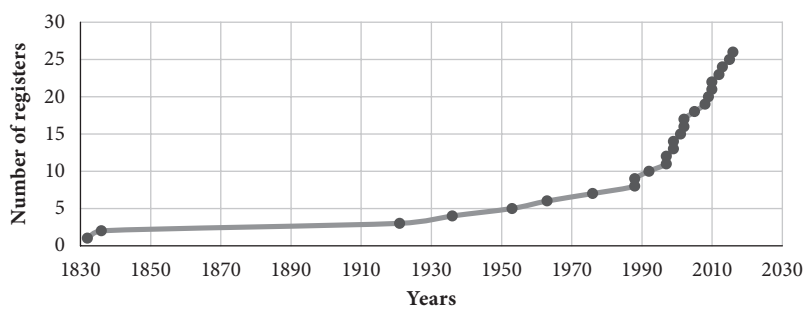
Keywords

Public register, personal data, privacy protection, government, processing, open, transparency.

I. The Growth of Public Registers

Public registers serve a variety of societal interests and have been in existence for centuries.[3] In the Netherlands, among the oldest national registers still operative today are the land registry (*Kadaster*, 1832) and the companies register (*Handelsregister,* 1921). These and other public registers are created and operated based on specific laws. The number of registers has grown slowly for a century and a half, only to explode in the past 20 years or so (see Figure 8.1). In part this is caused by EU law. Various recent and planned registers are the direct result of EU Directives, including the register of interpreters and translators and the forthcoming ultimate beneficial owners register.[4] The majority of recent registers involve the (online) publication of names of natural persons active in certain professions. The upward trend seems to continue. Currently discussed in Dutch Parliament are, among others, registers for mediators,[5] ultimate beneficial owners of legal persons,[6] fireworks experts[7] and professionals in building quality assurance.[8]

Figure 8.1 Growth of public registers contaning personal data in the Netherlands



[3] E.g. some date back to the sixteenth century. See Anna Berlee, *Access to Personal Data in Public Land Registers, Balancing Publicity of Property Rights with the Rights to Privacy and Data Protection* (Eleven International Publishing 2018) 214–216.

[4] Article 5(2) Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, OJ L 280, 26; Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('Fourth Anti-money Laundering Directive'), OJ L 141, 73; Directive (EU) 2018/843 ('Fifth Anti-money Laundering Directive'), OJ L 156, 43.

[5] *Kamerstukken* II 2012–13, 33722, nr 2 (Legislative proposal Mediators Register Act).

[6] Act implementing the Market Abuse Regulation, Stb. 2018, 239.

[7] 'Wat Is Persoonsregistratie? | Persoonsregistratie | Arboportaal'. Available at: www.arboportaal.nl/onderwerpen/persoonsregistratie/wat-is (last accessed 18 August 2018).

[8] *Kamerstukken* II 2015–16, 34453, nr 2 (Legislative proposal Act quality assurance for building).

Virtually all public registers can now be accessed online, greatly enhancing the accessibility of (personal) information contained in them. For example, if anyone wants to know if an incapacitated person domiciled in the Netherlands is under legal guardianship, all it takes is to key in last name and date of birth in the online register. Curious as to whether your local doctor has been subject of disciplinary measures? Simply download a list from the healthcare providers' register. Wondering how many square metres your boss' apartment is? The national building and addresses register returns data on size, type of dwelling, building year and a unique identifier (enabling access to ownership data in the land registry), if one performs an address search or uses the map tool.

Registers must comply with privacy and data protection law, in the EU especially with the GDPR and national implementing legislation.[9] There is no comprehensive research on whether they do. It may seem reasonable to assume that privacy and data protection concerns are consistently addressed by policymakers at the design stage of registers. An exploratory survey of the legislative record raised doubts as to whether this is indeed the case. On the basis of the exploratory research, we hypothesised that governments and lawmakers (a) easily assume that public registers serve their intended purposes and that these purposes justify the disclosure of personal information, and (b) rarely adequately assess their effectiveness and actual impact on privacy. We then did an extensive survey of official records on Dutch public registers. What does the legislative record show about if and how Dutch authorities weigh the purposes served by a public register against the right to privacy and data protection? The relevant laws at the fundamental rights level include Article 10 of the Dutch constitution, Article 8 ECHR and, for EU-based law, also Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU).[10] The relevant data protection laws are the General Data Protection Regulation and prior data protection laws.[11] When looking at if and how privacy interests were considered, the focus was on requirements of proportionality that flow from the fundamental right to privacy and the GDPR. What we found is that the official record, if at all, often shows evidence of a very superficial balancing of privacy interests, ex ante or ex post.

An in-depth description of all the characteristics (legal, operational, technical) of all public registers is outside the scope of this chapter. We will highlight some design aspects because the way in which (personal) information is disclosed affects the potential for privacy harms. Other data protection aspects (ie on data security, the rights of data subjects or enforcement) are not discussed.

[9] GDPR does not apply eg to data processing in the sphere of criminal justice and crime prevention (see Art 2(2)), but in this field registers are usually not public.

[10] Charter of Fundamental Rights of the European Union, OJ C 2012/326, 391.

[11] The Dutch constitution guarantees protection of the right to private life and this includes informational privacy. In legal practice Art 8 of the ECHR dominates because under Dutch constitutional law, treaties are hierarchically above national law (and provisions with direct effect can be invoked against application of domestic laws), and because Dutch courts are barred from assessing the constitutionality of legislation (Article 120 Dutch Constitution).

The chapter is structured as follows. After first explaining concepts and methodology (Section II), we elaborate on the requirement of proportionality (Section III). Section IV discusses findings of the empirical research for four categories of public registries in more depth. Section V concludes.

II. Concepts and Methodology

This section gives background to the (legal) concepts used and the methodology for the empirical research. With respect to concepts, we delineate what we mean by public registers and explain how these can be categorised on the basis of public interest goals pursued (II.A). Next, Section II.B sets out how the inventory and selection of public registers was constructed, and which resources were used for the analysis. Finally, in Section II.C we reflect a little more on the public nature of registers and what this means in a networked environment before we take a closer look at proportionality requirements in Section III.

A. Public Registers and their Purposes

For our purposes, the term public registers denotes: *systematic collections of information, that are accessible to the (general) public, held by public authorities, contain personal data and are intended to provide (some) information on natural persons*. For this chapter we studied 27 such national registers. There are many more registers held by public authorities, but personal information in those is either incidental or not publicly available (see Section II.B on selection). The idea was that for registers *designed* to give *public* access to *personal* information, one is more likely to find evidence of reflection on the need for these registers, on their effectiveness and on balancing potential privacy and data protection harms. If little attention was given to privacy and data protection interests in the design and operation of these registers (and, as noted, our exploratory research indicated that this is indeed the case), it seems likely that this is even less so for other registers. Of note, the fact that a public register does not fit our definition does not mean it has no bearing on privacy. Registers such as the abovementioned building and addresses register (which does not contain names of persons, or person identifiers), may have privacy implications because data from it can be combined with other public information, such as title to real estate from the Land Registry and thus enable identification of an individual.

Broadly speaking, the primary goal served by public registers studied here can be categorised as promoting:

(1) Accountability in the public sector: registers that help ensure the integrity of public offices, (eg through disclosure of ancillary positions of court officials, government ministers, registers of gifts and donations received by Members of Parliament).

(2) Economic and social transparency: registers that promote legal certainty in (commercial) transactions, attenuate information asymmetries between market actors (market regulation) and/or help maintain quality standards in a particular domain (eg healthcare).

These purposes have been assessed on the basis of relevant regulations and legislative records of the selected registers. These were then grouped according to similarity of purpose, as this allowed for a higher-level assessment of proportionality aspects. We will elaborate on these categories in Section IV.

B. Methodology

With respect to the survey, an initial set of 300 registers were identified by searching for legal instruments that regulate registers. The Dutch legislator itself recognises that a specific legal basis must exist for registers containing personal data.[12] Since legislative and parliamentary records and all legislation in force is accessible online (dating back to 1815), this produced a complete picture.[13] Further searches of key websites across government were carried out in the event not all public registers turned out to be regulated through (delegated) legislative acts or mentioned in the parliamentary records.[14] The resulting set was then validated against the Dutch government's own inventory, which can be found on the website of the Dutch Government Reference Architecture (*Nederlandse Overheid Referentie Architectuur – NORA*).[15] No additional registers were identified. The set was narrowed down to exclude those registers in which the inclusion of personal data is incidental. The set was then reduced further by considering only those registers that are publicly accessible. The latter means that registers to which access is limited to 'privileged parties' were excluded, like the central credit information system *CKI*. Also excluded were registers that limit access through technical design, for example, by requiring the keying in of detailed data that are only available to select people (ie unique identifiers combined with other attributes such a date of birth).[16] The resulting list contained 27 registers.

The question if and how the legislature weighs the societal interests of public registers was answered by looking at official parliamentary records. A caveat is in order here. The records do not necessarily give a full picture: it is conceivable,

[12] *Kamerstukken* II 2008–09, 31896, nr 3 (Explanatory memorandum alcolock programme).

[13] Official publications include legislative proposals, explanatory memoranda, reports of legislative debates in both houses of parliament (plenary, committee meetings), parliamentary questions, motions, references to external reports, etc.

[14] These are the websites of all Dutch Ministries, umbrella bodies of decentralised government entities (eg the Association of Netherlands Municipalities and Interprovincial Consultative Committee), the land register, and the Dutch Government open data portal data.overheid.nl.

[15] NORA, 'NORA Online'. Available at: www.noraonline.nl.

[16] An example is the register of certification for drivers of (construction) cranes, the 'TCVT' register, see www.tcvt.nl/persoonsregister/item12. To access it one needs to enter a unique crane driver certificate number and the date of birth of the holder of the certificate.

for example, that White Papers or external advice have informed public register legislation but that these documents were not sent to Parliament. In those circumstances it cannot be confidently established if proper consideration was given to questions of effectiveness and/or proportionality. Rather, the issue becomes one of transparency and accountability: should it be visible to the public that privacy interests have been considered?

It is a general principle that the processing of data must be transparent for the data subject (Art 5(1) GDPR) and that the processor is accountable for such transparency (Art 5(2) GDPR). But the GDPR does not, of course, explicitly require that considerations of proportionality are reflected in the legislative record on public registers. The GDPR does not require that a data protection impact assessment carried out by or for a public authority be publicly disclosed. Nor do the specific transparency requirements in Articles 13 and 14 GDPR require publication. The GDPR does provide for general principles on transparency of processing and the purposes of processing.[17] Transparency is highly desirable as it promotes the legitimacy and accountability of government actions, also with respect to compliance with data protection laws.[18] This has also been recognised by the Dutch Senate in 2011, when it carried a motion asking government to ensure that any legislative proposal with privacy implications is accompanied by an explanatory memorandum addressing the need, effectiveness and proportionality of the measures proposed.[19]

It is fair to assume that since public registers almost invariably are instituted by formal legislative acts (ie adopted by Parliament), certainly ex ante privacy concerns are reflected in the legislative record. Of note, older registers may predate data protection legislation, and this explains why the relevant original records do not show there has been debate on the privacy implications. But as will be detailed below, most registers are recent.

C. Publicness in a Networked Society

The digitisation of paper-based public registers, the growth in digital registers and the widespread availability of fast internet connections has changed the 'publicness' of registers. From systems of practical obscurity, where one had to physically go to a government office or request documents via post, they have evolved to systems of ubiquitous access, worldwide and instantaneous.[20] Of course, technical

[17] Artice 5(1)(a) and (b) GDPR. The principle of fairness in Art 5(1)(a) GDPR also supports transparency in the broadest meaning: Jef Ausloos, 'Giving Meaning to Lawfulness under the GDPR – CITIP Blog' (2017). Available at: www.law.kuleuven.be/citip/blog/2761-2/ (last accessed 17 February 2019).

[18] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2016) WP 260 6.

[19] *Kamerstukken I* 2010–11, 31051, nr D (Motion Franken).

[20] Berlee (n 3) 214–216; College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens Op Internet' (2007) 3.

means can be used to limit access, for example by using authentication technologies to reserve access to certain specific user groups, by geo-blocking or the use of APIs that prevent large-scale extraction of data. They matter when it comes to protecting privacy. Because we are primarily interested in how public goals served by registers are weighed ex ante against privacy interests, we do not detail how specific registers provide access to personal data. The selection of registers is of *public* registers, and the tendency among Dutch public authorities is not to restrict access.

The creation of public registers has become a standard policy tool since the 1990s. It is not just digitisation that drives this trend, but also new public management policies that see 'transparency' as an effective tool for quality control in (notably) regulated professions and semi-public domains. Furthermore, open government and open data policies at national and EU level promote the wide availability of public sector information. 'Open government' is a rather loose concept, or perhaps better seen as an ideal to make governments 'transparent, more accountable, and more responsive to their own citizens'.[21] An important instrument in open government policy is open government data: making data available to all is thought to promote 'transparency, accountability and value creation'.[22] This notion has gained considerable traction globally and in the EU.

The 2013 Public Sector Information Directive[23] has been revamped into the Open Data and Public Sector Information Directive. It tightens the rules that must ensure more public sector data becomes available for (commercial) reuse by default. It must be implemented by Member States in 2021.[24] Data protection laws and privacy rights must be respected when releasing data for reuse (eg by anonymisation). This assessment tends to be done on a case-by-case basis: does release of this particular data set or using this particular API on that particular public register satisfy data protection rules? The Public Sector Information Directive and the GDPR do not focus on systemic effects that arise when ever more resources become available online, in machine-readable, open formats, which greatly facilitate the linking of data from different sources. Open data policies are designed to promote just that development.

Publication of personal data in a register can have varying effects on the private life of the persons concerned. Names, addresses and unique identifiers from

[21] See the mission of the Open Government Partnership (an international initiative joined by nearly 80 countries including EU Member States). Available at: https://www.opengovpartnership.org/mission-and-strategy/.

[22] See, for the involvement of the OECD: www.oecd.org/gov/digital-government/open-government-data.htm and United Nations: https://publicadministration.un.org/en/ogd.

[23] Mireille Van Eechoud and Corien Prins, 'Directive on Public Sector Information Re-Use' in Serge Gijrath and others (eds), *Concise European Data Protection Law, E-commerce and IT Law* (Kluwer Law International 2018).

[24] Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information, COM/2018/234 final (file 2018/0111(COD)). Adopted by Council and European Parliament (Adopted P8_TA-PROV(2019)0352 on 04/04/2019).

public registers enable third parties to engage in direct marketing but also facilitate significant harms, like identity theft or the making of direct threats.[25] Combining data from public registers with information from other sources may help profiling.[26] The possibility to combine information exacerbates risks, meaning that governments should not assess the impacts of disclosure of personal data in public registers on (just) a case-by-case basis.

That information is accessible *online* has additional privacy implications, as the Court of Justice of the EU (CJEU) noted first in *EDate* and then in *Google Spain*. The fact that (injurious) information is available on a world-wide basis can aggravate the privacy harm.[27] The persistence of information on the internet once released is another factor. Also, that information is publicly available in registers does not mean that subsequent publications are unproblematic. In *Satakunnan Markkinapörssi Oy & Satamedia Oy v Finland*, the European Court of Human Rights (ECtHR) held that the use of already public information on a much larger scale can in itself constitute an interference with the right to private life.[28] In this case, the availability of personal data through a text messaging service was considered an interference with the right to private life, even though this information was readily available at local administrative offices.[29] In *Satakunnan*, 'downstream' companies using data from public tax records were the offending party (the Finnish data protection authority and courts had issued orders to desist). While the Court did not have to consider the role of government, it does show that governments may limit re-use of public data if personal data is concerned.

III. Requirements of Proportionality

In this section we look to key principles of the GDPR (or equivalent principles from its precursor Directive 95/46/EC) that are the most relevant for public registers. First, the principle that personal data may only be processed if it complies with one of a limited number of *lawful grounds*; second, that the *purpose*(s) for which processing takes place is legitimate; and third, that such processing (in our setting: public disclosure) is *necessary* to achieve the stated purposes. The 'necessity' requirement will function as a key for applying proportionality standards from

[25] Maeve McDonagh, 'The Protection of Personal Information in Public Registers: The Case of Urban Planning Information in Ireland' (2009) 18 *Information & Communications Technology Law* 19, 21; Joost Schellevis, 'Gegevens KvK-Inschrijvingen Gebruikt Voor Reclames Op Facebook | NOS' *NOS* (18 April 2018).

[26] McDonagh (n 25) 21.

[27] Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50, para 80, referring to Joined Cases 509/09 and C-161/10 *eDate Advertising a.o.* ECLI:EU:C:2011:685, [2011] ECR I-10269, para 45.

[28] *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [GC], no 931/13, ECHR 2017 (extracts), para 98.

[29] Ibid, para 134.

Article 8 ECHR and Articles 7 and 8 of the EU's Charter of Fundamental Rights (CFREU) in the GDPR.

A. Lawfulness for Public Register Processing

Lawmakers must establish a lawful ground for the processing of personal data in registers. That lawful ground must also cover publication. Two of the GDPRs lawful grounds are of particular relevance to public registers: compliance with a legal obligation (Article 6(c) GDPR) and performance of a task carried out in the public interest or exercise of official authority (Article 6(e) GDPR).[30] As to the first, the law that imposes the legal obligation must fulfil 'all conditions to make it valid and binding and in compliance with data protection law, including necessity, proportionality and purpose limitation'.[31]

In the absence of a legal obligation, institutions may be able to rely on Article 6(e) GDPR if publication is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.[32] The Article 29 Working Party (the EU's former advisory body of representatives from all national data processing authorities) has stated that institutions will need to consider the public interests served, whether processing is appropriate for attaining the objective pursued and that they further will need to 'bear in mind the various interests at stake'.[33] This suggests proportionality must be assessed.

The legal grounds in Articles 6(c) and (e) overlap to some extent. According to the Working Party, processing based on the (e)-ground should be directly or indirectly based on a legal provision.[34] Furthermore, the Working Party argued that if the processing implies an invasion of privacy, this legal provision should be specific and precise, detailing the data processing allowed under it.[35] Such a legal provision would then also be a legal obligation within the meaning of Article 6(c). However, the Working Party has stated on a different occasion – in its opinion on legitimate interest – that public interest or official authority is 'typically attributed' through statutory or other laws.[36] This could mean that it does not exclude the possibility of processing based on Article 6(e) GDPR in absence of a (specific) legal

[30] According to Article 29 Working Party, the most important legal basis for the publication of personal data for transparency purposes is Art 6(c) GDPR. The Dutch DPA also expects that this ground will increasingly be used by public and private parties mandated by law to maintain public registers. See: Article 29 Working Party, 'Opinion 02/2016 on the Publication of Personal Data for Transparency Purposes in the Public Sector', 2016, 5; College Bescherming Persoonsgegevens (n 20) 23.

[31] Article 29 Working Party, 'Opinion 8/2014 on the Notion of Legitimate Interests of the Data Controller', (WP 217) 2014, 19.

[32] Article 29 Working Party, 'Opinion 02/2016 (n 30); Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18, para 42.

[33] Ibid.

[34] Article 29 Working Party, Opinion 02/2016 (n 30) 5.

[35] Ibid.

[36] Article 29 Working Party, Opinion 8/2014 (n 31) 22.

obligation, but only if the processing of personal data does not imply an invasion of privacy in the sense of Article 8 ECHR.

Consent could, in theory, be a further legal ground, but will be problematic in most cases.[37] After all, public disclosure is often based on statutory laws that oblige the data subjects to provide data (eg land registry, commercial register, health care providers' register).[38] Even without a legal obligation, to provide data 'voluntarily' or agree to its disclosure will not normally meet the strict standard that the GDPR sets for consent.[39] Consent may be undermined by the negative consequences of not agreeing to provide and disclose personal data (eg if economic duress results).[40] But there may also be cases where consent is an appropriate ground. For example, while interpreters are obliged to register with the Dutch register of interpreters (without registration interpreters will not be hired by large parts of government, including the police, public prosecutor's offices and courts),[41] they are free to refuse public disclosure of their data.

B. Necessity as Proportionality

Processing personal data is bound by a legitimate purpose that must be specified before processing commences.[42] A legal provision mandating disclosure as such does not constitute a legitimate purpose; the GDPR requires a specific purpose for the register legitimising the legal provision mandating a public register. For example: the ancillary jobs register of judges is based on Article 44a of the Act on the Legal Position of Judicial Officers.[43] Its purpose lies in ensuring judicial independence and impartiality, and public trust in the judiciary.[44] Considering the importance of trustworthy, impartial courts for the rule of law, these purposes are legitimate within the meaning of the GDPR. The requirement of 'necessity' is central to the assessment of the legitimacy of processing for Articles 6(c) and (e) GDPR.[45] 'Necessary' presupposes that maintaining a public register is in fact

[37] Since the entry into force of the GDPR, it is not or no longer possible for public authorities to rely on the lawful ground of legitimate interest when processing is in the performance of their tasks, see Art 6(f) and final sentence GDPR.

[38] Anna Berlee, 'Volledige Openbaarheid: Het Doel Voorbij' (2017) 2017 *WPNR* 844, 848.

[39] F Zuiderveen Borgesius, M Van Eechoud, and J Gray, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30(3) *Berkeley Technology Law Journal* 1–32; Article 29 Working Party, 'Opinion 01/2012 on the Definition of Consent' (WP 187) 2011, 12–13.

[40] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, Opinion of AG Sharpston, paras 82–83.

[41] Article 28 Sworn Interpreters and Translators Act (*Wet Beëdigde Tolken en Vertalers*), Stb 2007, 471.

[42] GDPR recital 39.

[43] Art 44a *Wet Rechtspositie Rechterlijke Ambtenaren.*

[44] *Kamerstukken II* 1994–95, 24220, nr 3 (Explanatory Memorandum).

[45] This requirement of 'necessity' is central to the assessment of the legitimacy of processing for Arts 6(c) and (e) GDPR, see: Frederik J Zuiderveen-Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Wolters Kluwer Business 2015) 143.

needed for the controller to meet a legal obligation under Article 6(c) GDPR, or to properly exercise a public task under Article 6(e) GDPR.

According to the Article 29 Working Party, the ECtHR approach to 'necessity' should be adopted in the context of the lawful grounds for processing.[46] Under Article 8 ECHR, the proportionality principle follows from the ECtHR's interpretation of the requirement that an interference with the right to private life has to be 'necessary in a democratic society'.[47] The classic three-part proportionality test that the ECtHR applies for all human rights requires (1) that interests have been balanced, (2) that the processing is a suitable means to attain the underlying legitimate (policy) purpose(s) and that (3) the least intrusive means are used.[48] The first two parts will be discussed further below. In a nutshell, the purpose specification and balancing of interests must take place before public disclosure commences.[49] Furthermore, suitability means that public disclosure has to be an effective instrument to obtain the legitimate purpose; an ineffective policy will not be proportionate to the interference it poses.[50] The availability of less intrusive means is less relevant for this study, as it concerns mostly the choices for precise instruments.[51] This step in the analysis focuses more on specific implementation issues (eg modalities of access through restrictive APIs) and not the broader discussion on whether public disclosure as such is proportionate.

The requirements of proportionality apply not only to Article 8 ECHR, but also the right to private life under Article 7 CFREU. Limitations to this right are subject to the general principle of proportionality enshrined in Article 52(1) CFREU. Additionally, Article 52(3) CFREU explicitly states that the meaning and scope of rights corresponding to those guaranteed in the ECHR should be the same as those laid down by said Convention.

It is debatable whether the requirements for proportionality in Article 8 ECHR also apply to the data protection right. Protection of personal data can be construed as part of the right to privacy of Article 8 ECHR in cases where

[46] Article 29 Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211 13–14. See also Article 29 Working Party, Opinion 02/2016 (n 30) 5. Also arguing that the term 'necessary' directly reflects the proportionality principle of Art 8 ECHR: JAG Versmissen and ACM De Heij, 'Elektronische Overheid En Privacy', (2002) 25 *Achtergrondstudies En Verkenningen* 37.

[47] CBP, 'Actieve Openbaarmaking En Eerbiediging van de Persoonlijke Levenssfeer' (2009) 5; Zuiderveen-Borgesius (n 45) 143.

[48] Janneke Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466, 469.

[49] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, para. 85. See also GDPR, recital 39.

[50] Charlotte Bagger Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 *International Data Privacy Law* 239. See also as applied in Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland*, ECLI:EU:C:2014:238, [2014] 3 CMLR 44, paras 49–52.

[51] Gerards (n 48) 470.

processing interferes with privacy interests.[52] But not all personal data processing affects privacy. Since the right to data protection of Article 8 CFREU has no equivalent in the ECHR, this suggests the extended application of the ECHR through Article 52(3) CFREU does not apply. However, the *Handbook on European Data Protection Law* issued by the European Union Agency for Fundamental Rights and the Council of Europe states that the proportionality principles applicable to data processing are reminiscent of Article 8(2) ECHR.[53] We therefore assume that proportionality for the data protection right also follows the classic three-part proportionality test.

i. Proportionality as Effectiveness

Embedded in the lawful processing grounds is a requirement that the processing (ie operation of the public register) is an effective means to achieve the purpose it serves. In their report to the Dutch Data Protection Authority, Versmissen and De Heij argue that the legislator should take account of the effects of their policies to assess whether the intended purpose of a public register is actually achieved.[54] It is, therefore, important to assess what is known about the effectiveness of the various public registers. An absence of effectiveness in reaching the legitimate purpose pursued indicates a disproportionate interference in the right to private life and personal data protection.

This approach also finds support in the case law of the CJEU. In *Digital Rights Ireland*, the referring domestic court queried whether the Data Retention Directive, requiring storage of all telephone traffic and location data, was not just disproportionate, but also inappropriate to achieve the aims pursued.[55] The CJEU answered that proportionality entails, among others, that the interference need to be appropriate for attaining the legitimate objectives pursued.[56] Applied to public registers, the disclosure of personal data must be suitable for attaining the desired policy purpose. That is: if a measure does not provide actual opportunities to achieve the public interest (ie it is not effective) it cannot be seen as an appropriate tool to attain the objective.[57] This is also evident from the CJEU's *Huber* case,[58] which revolved around the question whether plans to centralise pre-existing population registers are 'necessary' to facilitate application of residential

[52] Anna-Sara Lind and Magnus Strand, 'A New Proportionality Test for Fundamental Rights ?' (2011) 1 *European Policy Analysis* 6.

[53] European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Data Protection Law* (2014) 67.

[54] Versmissen and De Heij (n 46) 37.

[55] Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland*, ECLI:EU:C:2014:238, [2014] 3 CMLR 44, para 18.

[56] Ibid, para 46.

[57] Ibid, para 49, where the CJEU concluded that the Data Retention Directive allowed national authorities to shed light on serious crimes and may consequently be considered to be appropriate.

[58] Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724, para 62.

laws and for statistical purposes.[59] The Court held that this is so if 'its centralised nature enables that [residence] legislation to be more effectively applied …'[60]

ii. Proportionality and Balance of Interests

A public register should not only be appropriate to obtain the objective, but also proportional in the strict sense: the balance of interests must fall in favour of the purpose served by public disclosure. It is difficult to discern substantive criteria for proportionality as a reasonable balance between the interference and the rights to private life and personal data protection. Case law of the ECtHR and CJEU are very context specific, relying heavily on suitability and least interfering means instead of a more abstract balance of rights and interests.[61] Still, the CJEU concluded in the case of *Volker und Markus Schecke and Eifert* – on the publication of the names of recipients of EU agricultural subsidies – that institutions are obliged to balance the interests prior to disclosure.[62] This has also been stressed by the Dutch Senate. Just after publication of the *Volker und Markus Schecke and Eifert* case, the Senate carried a Motion that explanatory memoranda to legislative proposals should contain, inter alia, information on necessity, effectivity, proportionality, and the results of a data protection impact assessment.[63]

The need to take the interests of data subjects into account at an early stage also follows from new norms introduced by the GDPR. Data protection by design and by default, as introduced in Article 25 GDPR, obliges the controller to implement appropriate measures at the time of the determination of the means for processing. Furthermore, the controller should carry out an ex ante data protection impact assessment if data processing is likely to result in a high risk to the rights and freedoms of natural persons.[64] This should contain an assessment of the necessity and proportionality of the processing in relation to the purposes.[65] Whilst the assessment is not always mandatory, the Dutch Government has opted to perform such an assessment in all cases where the development of new policies and regulations concern the processing of personal data.[66] As already discussed in the section on methodology, a caveat to these new rules is that there are no requirements to publish the results of data protection by design and impact assessments.

[59] Art 7(e) Data Protection Directive, equivalent to GDPR, Art 6(e).

[60] Ibid. A further condition is that the register 'contains only the data which are necessary for the application by those authorities of that legislation'. The Court did not accept that a centralised register is necessary for statistical purposes.

[61] Manon Oostveen, *Protecting Individuals Against the Negative Impact of Big Data: Potential and Limitations of the Privacy and Data Protection Law Approach* (Wolters Kluwer 2018) 87–88.

[62] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, paras. 83, 85.

[63] *Kamerstukken I* 2010–11, 31051, nr D (Motion Franken).

[64] GDPR, Art 35.

[65] Ibid, Art 35(7)(b).

[66] Ministry of the Interior and Kingdom Relations, 'Model Gegevensbeschermings- Effectbeoordeling Rijksdienst (PIA)' (2017) 6.

An important aspect to the balance of interests is the question whether publication should necessarily be in the form of an online publication. The Article 29 Working Party argues it is necessary to consider the potential risk of online disclosure.[67] The Dutch DPA insists that public bodies should reflect on the question whether publication should always mean publication on the internet.[68] An obligation to publicly disclose personal data does not automatically mean that it should be available online,[69] let alone in a form that allows easy bulk retrieval. Offline access comes with practical limitations which may limit the extent to which data is actually disseminated. Online availability without strict access limitations may lead to a much wider distribution, even if this is not strictly necessary to achieve the register's purposes. Furthermore, online accessibility facilitates the combination of personal data from multiple sources. This means that there can be further proportionality issues with online publications. This is especially important for registers that have existed since before the advent of the internet and are now increasingly migrated online.

If we look to Dutch Government practice, disclosure of data in public registers can range from online publication of datasets in downloadable CSV- or XML-format, to more limited disclosures through APIs, requiring input of last names or other identifiers. How robust such technical measures are is another matter. A 2017 study found that many registers that list professionals for purposes of qualification checks actually provide more data than is needed to check their qualifications.[70] Researchers used wildcards and SQL-injects to obtain the complete dataset of registered doctors in the Dutch health care providers (so-called '*BIG*-register') and other registers maintained by government.[71]

IV. Types of Public Registers and their Purposes

Above we identified two broad categories of purposes of public registers. The first category is primarily concerned with ensuring (political) accountability of public institutions and, through such openness, promote trust in the legislature, judiciary and executive branches of government. Registers in this category are concerned mostly with the integrity of public offices. The second broad category is concerned with economic and social domains: to promote legal certainty in (commercial) transactions and attenuate information asymmetries between market actors (market regulation), and/or help maintain quality standards in a particular domain. Here we discuss in a little more detail examples of registers

[67] Article 29 Working Party, 'Opinion 02/2016 (n 30) 8.
[68] College Bescherming Persoonsgegevens (n 20) 41.
[69] Ibid 23.
[70] Sjoerd Van der Hoorn, 'Gegevensopstraat.Nl'. Available at: www.gegevensopstraat.nl/ (last accessed 17 August 2018).
[71] Ibid.

in both categories and the extent to which their creation and further existence is supported by sufficient privacy and data protection considerations.

Of note, public registers may predate modern data protection norms following from the GDPR and its predecessor, the European Data Protection Directive 95/46/EC. The Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) of 1998 implemented Directive 95/46/EC and also applied to public registers. The earlier Data Protection Act of 1989 (*Wet Persoonsregistratie*), however, explicitly excluded public registers from its scope. The explanatory memorandum to that Act stated that the law should not apply to registers because 'in these cases, the legislator has decided that these registers are intended for publicity.'[72]

A. Accountability in the Public Sector

Dutch public registers on government transparency that disclose personal data are mostly registers on ancillary jobs held by politicians and judges. These are the ancillary jobs registries for Members in both houses of Parliament, the European Parliament, the Provincial Executive, the board of the *Waterschappen* (regional authorities tasked with water management), mayors and aldermen and judges.[73] In addition, publication is required for gifts and foreign travels subsidised by third parties for politicians in the *Tweede Kamer* (Lower House of Parliament).[74] Most of these registers have existed for quite some time, but have only fairly recently been regulated in (delegated) acts. For example, the publication of ancillary jobs for Members of parliament exists since 1976 but was only formalised in the rules of procedure (*Reglement van Orde*) in 2002.[75]

i. Purposes

Two arguments recur in the parliamentary record: to prevent conflict of interests or the appearance of such conflict, and to assess whether an ancillary job compromises the exercise of a public function.[76] There has been some discussion in Parliament on the need to balance privacy interests of registered persons with transparency interests,[77] but hardly any on later decisions to make the registers

[72] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet persoonsregistratie*), 18; Art 2(2) Persons Registration Act.

[73] See Art 5 *Wet Schadeloosstelling leden Tweede Kamer* and Art 150a *Reglement van Orde Tweede Kamer*; Art 3b *Wet vergoedingen leden Eerste Kamer* and Art 256d *Reglement van Orde Eerste Kamer*; Art 6 *Wet Schadeloosstelling, uitkering en pensioen leden Europees Parlement* (Stb 2010, 122); Art 40b *Provinciewet*, Art 41b *Gemeentewet*, Art 44a *Waterschapswet* (Stb 2010, 110); and finally Art 44a *wet rechtspositie rechterlijke ambtenaren* (Stb 1996, 590).

[74] Art 150a *Reglement van Orde Tweede Kamer*.

[75] *Handelingen* II 2002–03, nr 62, 3719.

[76] *Kamerstukken* II 2005–06, 30425, nr 3 (Explanatory Memorandum).

[77] *Kamerstukken* II 2004–05, 29937, nr 3 (Explanatory Memorandum); *Kamerstukken* II ibid.

freely available online. For example, the legal history of the judges' register merely states that the register should be placed on the internet because trust in the judiciary benefits from maximum publicity.[78] It does not provide any reasoning on what this 'maximum publicity' may entail for data subjects.

ii. Effectiveness and Proportionality

With respect to effectiveness of the register, the absence of evaluations is conspicuous. Only the judges' register has been evaluated, but that did not include questions of effectiveness of the disclosures in relation to the interferences with privacy and data protection.[79] The evaluation reported that registers maintained by local courts were often incomplete, outdated or merely described an ancillary job vaguely, such as 'member of a Supervisory Board'.[80] The register was centralised and standardised in reaction to the evaluation, to provide greater transparency.[81] News magazine *De Groene Amsterdammer* reported similar issues for the registers of public officials in decentral government.[82] As such, it seems that these registers are sparsely regulated. There is some anecdotal evidence that the media use the jobs registers; for example, newspaper *Brabants Dagblad* regularly advertises any ancillary jobs such as mayor in the Brabrant province.[83] However, the absence of publicly available information of the suitability of these registers makes it impossible to assess whether they are actually proportional.

B. Economic and Social Transparency

In this broad domain we find registers that promote legal certainty in (commercial) transactions and attenuate information asymmetries between market actors (market regulation) and/or help maintain quality standards in a particular domain. Based on the type of information contained, a further distinction can be made in registers focusing on:

- professional qualifications
- financial information and
- legal representation of persons and companies.

[78] *Kamerstukken* II 2004–05 ibid.
[79] RJJ Eshuis and N Dijkhoff, 'Nevenfuncties Zittende Magistratuur', (2000) *Onderzoek En Beleid* 185.
[80] Ibid, 58, 60.
[81] *Handelingen* II 2002–03, *aanhangselnummer* 7 (24 September 2002).
[82] Erik Van Rein, Erik Verwiel and Marlie Van Zoggel, 'Het College Klust Bij' [2017] De groene Amsterdammer.
[83] 'Burgemeester Wikt, Weegt En Zegt Die Ene Bijbaan Op,' *Brabants Dagblad*, 16 November 2017; 'Bijbaan Voor de Burgemeester', *Brabants Dagblad*, 23 February 2017.

i. Professional Qualifications

The registers dealing with professional qualifications have grown considerably in numbers the past decades. Of 15 registers, 13 date from the late 1980s and six were created this last decade, long after EU data protection law was in place.

(a) Purposes

A particular register may be informed by subsets of goals. For example, the register of health care providers such as doctors, nurses, physiotherapists and dentists serves more than one purpose. It informs (prospective) patients on who is qualified to provide a certain service. This attenuates information asymmetries. But the register is also supposed to help maintain quality standards in the regulated professions. In order to keep a valid registration, health care providers must show evidence of continued training and comply with other quality standards. The disciplinary measures taken against health care providers are also publicised, not only to warn patients (and prospective employers, health insurance companies and the like), but also to act as a punishment. In fact, many of the public registers on regulated professions serve such a mixture of these three goals.

An exception to the rule that public registers have a clear legal basis is the 'social hygiene register'. The Minister of Health should have appointed an organisation to maintain a register of workers in hospitality with food and drink safety certificates and regulate it.[84] The examination board for social hygiene certificates *LEC-SVH* took up the task, without having been officially appointed.[85] The register is currently accessible to everyone, although the law stipulates that it is meant only for relevant civil servants and mayors. The legislative record states that the Minister will make a privacy assessment, but there is no clear sign that this has been done.[86]

(b) Effectiveness and Proportionality

The situation for the category of 'professionals registers' is quite typical of results found for other registers. In half the cases, the legal history is silent on the relation between the purpose of the register and privacy and data protection. This is true for the auditors register, the architects register, the social hygiene register and the bailiffs register. Some of these pre-date the European data protection norms and the earlier Dutch Persons Registration Act of 1989 (*Wet Persoonsregistratie*) categorically excluded public registers from its scope.[87] All that can be found in the

[84] Alcohol and Food Service Industry Act, Art 8(5).
[85] Heinrich Winter, Bieuwe Geertsema and Erwin Krol, 'Evaluatie LEC-SVH' (2016) 9.
[86] *Kamerstukken* II 2008–09, 32022, nr 41 (Third rectifying letter).
[87] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet Persoonsregistratie*), 18; Persons Registration Act, Art 2(2).

legal history of the notaries register is a statement that 'it goes without saying that the register must be public'.[88]

A number of older registers have been supplemented with a purpose specification (eg to inform interested parties) following the implementation of the Data Protection Directive, but without any further assessment of proportionality.[89] Of note, four registers created after the implementation of the Data Protection Directive still lack a visible assessment on purpose and proportionality.

For one-third of registers evidence of some balance of interests exists. On the register of forensic experts, the former Minister of Justice argued that disclosure should be based on consent of the registered persons (one may ask whether forensic experts are really free to withhold their consent, if doing so has economic ramifications),[90] and that disclosure is necessary to inform potential clients about experts' qualifications.[91] The same reasoning is used for the register of youth care professionals: public disclosure is deemed necessary to assess which professionals qualify for certain tasks.[92] As such, the human rights interferences of these registers are deemed proportionate as the only way for the public to ascertain the qualifications of professionals. However, this does not explain why enabling the public to ascertain the qualities is necessary for these professionals specifically, but not for other professions. That would come down to a political consideration on the societal value of specific professions, the public role they play and whether this publicity actually serves the public interest.[93] It also depends on the question to what extend citizens should be ascertaining these qualifications and not government institutions charged with safety in certain professions.

Public disclosure of disciplinary actions is also balanced in some cases. Disclosing disciplinary actions in the veterinary register is only deemed justified if it concerns a total or partial prohibition to practice veterinary medicine.[94] The central advocates register contains a similar balance.[95] The former Junior Minister of Justice Teeven argued that disclosing all disciplinary actions would result in a disproportionate interference with privacy.[96] Teeven argued that disclosure is

[88] *Kamerstukken* II 1995–95, 23706, nr 6 (Note on the report). The names of notaries were already disclosed to the public in the Government Gazette before the creation of a public register.

[89] See Art 3(5) *Wet op de Beroepen in de Individuele Gezondheidszorg; Kamerstukken* II 1999–2000, 26410 nr 8 (Rectification letter); TK II 1999-00, 26410, nr 3 (Explanatory Memorandum Amendment of provisions relating to the processing of personal data); Stb 2002, 336; Stb 2003, 159; *Kamerstukken* II 2000–01, 27193 nr 6 (Rectification letter).

[90] Decree on the register of forensic experts, Stb 2009, 330.

[91] Ibid.

[92] Decree to the Youth Act, Stb 2014, 441.

[93] *Kamerstukken* II 2010–11, 32382, nr 8 (Rectification letter); *Kamerstukken* II 2015–16, 34458, nr 4 (Advice Council of State and further report).

[94] *Kamerstukken* II 1982–83, 17646, nr 3 (Explanatory Memorandum).

[95] *Kamerstukken* II 2010–11, 32382, nr 8 (Rectification letter).

[96] Act on the status and oversight over the legal profession, Stb 2014, 354; Stb 2014, 429 (entry into force); *Kamerstukken* II 2010–11 (n 95).

only necessary for clients to assess whether certain advocates may still perform their profession.[97] The situation is very different with respect to the disclosure of disciplinary actions in the doctors register. In this case, all disciplinary actions are made public. The then Minister of Health, Schippers, argued that it ensures that patients, employers and stakeholders are better informed,[98] so the right to know must trump privacy and data protection interests.[99] This does not seem to be a weighing of interests, but merely a choice for the preferred policy.

Overall, formal evaluations and studies on the effectiveness of professional qualifications registers are rare. The healthcare providers' register is an exception. Research shows that patients hardly ever ask medical professionals about their registration.[100] Research carried out for the national medical sciences funding agency concluded that of the respondents who knew about the healthcare providers' register ($N = 542$), 83 per cent of respondents had never used it.[101] Eight per cent stated that they had used the register when choosing a new health care professional.[102] Of note, registration is seen as the least important factor when choosing a new professional.[103] Research institute Nivel questioned a larger group of respondents ($N = 862$) and concluded that a mere 1.4 per cent of respondents looked at the register when choosing a new health care professional.[104] This does not seem to be an impressive number, particularly as the register covers virtually all types of health care professionals, not just general practitioners (family doctors) with whom the patient may already have a long-standing relationship. Part of the stated goals discussed above is to promote quality of health care provision by empowering citizens with information. If, in effect, registers are used so little, one might ask if they are effective instruments.

ii. Financial Information

Another type of register provides financial information to promote legal certainty. These registers aim to reduce risks for potential contracting parties.[105]

[97] *Kamerstukken* II 2010–11 (n 95).

[98] *Kamerstukken* II 2014–15, 29282, nr 203 (Letter of the Minister of Health on labour market policy and education health care sector).

[99] EH Hulst, 'Naming En Shaming van Artsen Die Tuchtrechtelijk Zijn Veroordeeld' (2017) 1 *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 1.

[100] JG Sijmons et al., 'Tweede Evaluatie Wet Op de Beroepen in de Individuele Gezondheidszorg', Reeks Evaluatie Regelgeving, 2013, 53.

[101] Ibid.

[102] Ibid.

[103] Ibid at 54.

[104] Roland Friele et al., 'Zorgverleners En Burgers over Het Openbaar Maken van Door de Tuchtrechter Opgelegde Berispingen En Geldboetes' (2017) 35.

[105] These constraints also apply *erga omnes*, as opposed to limitations under contract law, meaning that registration can be invoked against anyone.

(a) Purposes

This purpose is not necessarily made explicit in the relevant regulatory instruments but can be inferred from the register's effect. The legal guardian register (*Curateleregister)* discloses who is legally incapacitated; the receivership register (B*ewindregister*) warns creditors about problematic debtors, meaning creditors unable to enforce their claims through a court procedure;[106] and the insolvency register (*Faillissementsregister*) informs creditors that natural persons no longer have power of disposition on their property.[107] Similarly, the prenuptial agreement register informs creditors about marital conditions, which may limit the power of disposition of one spouse regarding goods owned by the other spouse.[108] These registers all inform (potential) creditors about the restraints put upon the natural person they have or may want to have economic relations with. The legal restraints and receivership registers have the secondary function of protecting the registered subject from creating further debts.[109]

Public disclosure of the land registry similarly has the purpose of ensuring 'an equal information position between parties'[110] involved in real estate transactions. It details ownership, as well as mortgages and other security interests attached to a property.

Of a somewhat different nature are the two registers held by the Financial Markets Authority (*AFM)* with information on management owned shares and other financial products. Disclosure of such information has the purpose of minimising asymmetric information between managers, directors and supervisory directors and other (potential) shareholders.[111] This only promotes trust of (potential) shareholders and other investors in the company, but also functions as a remedy against insider trading.[112] These registers are, therefore, somewhat different than the others in this category as they seek to promote both a level playing field in the stock market and honest trading.[113]

(b) Effectiveness and Proportionality

The public records are almost completely silent on the privacy and data protection interests pertaining to financial information registers. Only with regard to the legal restraints and receivership registers does the legislative record state that privacy and date protection interests are outweighed. In these cases, disclosure is

[106] *Kamerstukken* II 2011–12, 33054, nr 6 (Note on the report).
[107] Insolvency Act, Art 23.
[108] Article 1:116 Dutch Civil Code; Article 1:121 in connection to Article 1:94 Dutch Civil Code.
[109] *Kamerstukken* II 2011–12, 33054, nr 3 (Explanatory Memorandum).
[110] IJ Kloek-tromp, 'Kadaster En Privacy in Praktijk' (2017) *WPNR* 854.
[111] *Kamerstukken* II 1996–97, 25095, nr 3 (Explanatory Memorandum); *Kamerstukken* II 2000–01, 27900, nr 3 (Explanatory Memorandum).
[112] Ibid.
[113] The legal title of Regulation 596/2014 imposing the publication of transactions by managers is aptly called the 'Market Abuse Regulation'.

also deemed to be in the data subject's financial interests.[114] The legal history of the insolvency register, the Land Registry, the register on shares and other financial products held by (supervisory) directors remain silent. The *AFM* register on transactions by managers would at first remain closed due to privacy interests, only to disclose it anyway 'to align the system with the Anglo-Saxon model'.[115] It is also questionable whether the purpose of this register is to provide information in trade at all or only to check upon illegal insider trading. Public disclosure would perhaps not be necessary in the second case, as long as the *AFM* remains informed.[116]

As to the effectiveness of the public registers, this does not seem to be questioned by lawmakers and policymakers. Legal certainty is certainly served by the Land Registry because registration of deeds is required for transfer of property to have effect. Other registers produce legal effects too (eg by limiting the ability of creditors to make certain claims in court).

iii. Legal Representation of Persons and Companies

A smaller but relatively old set of registers, these inform the public about their capacity to act on behalf of a natural or legal person (eg a company, foundation, association, etc.). The commercial register discloses the names of directors and other authorised representatives of a company.[117] The guardianship register details which persons (parents, guardians) have the legal power of representation over minors.[118] These registers provide legal certainty in trade by providing information on the representatives of a natural or legal person and related risk liability.[119] Legal certainty as a legitimate purpose for disclosure in commercial registers has been recognised by the CJEU in *Camera di Commercio v Manni*.[120] To improve his chances in business, Salvatore Manni sought to have information about prior bankruptcies removed from the commercial registers.[121] For this he relied on data protection law – including the 'right to be forgotten' as elaborated in *Google Spain and Google*.[122] The CJEU held that the publication of personal data was necessary for the commercial register to serve the purpose of legal certainty;[123] not just for creditors, but also for potential trade partners of other companies which Manni represented as a director.[124]

[114] *Kamerstukken* II, 2011–12 (n 109).
[115] *Kamerstukken* II 1997–98, 25095, nr 12 (Amendment Voute-Droste).
[116] However, public disclosure could in this case merit accountability of the *AFM*. This would have to be made an explicit and proportional purpose of the register.
[117] Art 2 Commercial Register Act (*Handelsregisterwet*).
[118] Article 1:244 Dutch Civil Code (*Burgerlijk Wetboek).*
[119] NORA (n 15); Berlee (n 38) 844.
[120] Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18.
[121] Ibid.
[122] Ibid; Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50, para 91.
[123] Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18, para 42.
[124] Ibid, para 63.

(a) Effectiveness and Proportionality

The public records show no evaluation or other research on the effectiveness of these registers. Registers preceding the Data Protection Act (*Wet Bescherming Persoonsgegevens*) generally lack a balancing of the public interest in disclosure and the rights to private life and personal data protection. This is also the case for the commercial register. The only mention made on necessity of disclosure at all is in 1983. Former Minister of Justice Korthals Altes argued that disclosure is necessary to have certainty about the natural persons that have decisional or representational authority over a company or other legal person.[125] No balancing of proportionality can be found in later amendments, including the amendment of 1997 which made the commercial register electronically accessible.[126] The explanatory memorandum to the overhaul of the Commercial Register Act in 2007 merely mentions that the Data Protection Directive applies to the Commercial Register.[127] It does not provide a discussion on the balance between data protection and disclosure in the public register.[128] As a matter of interest, The Dutch DPA (*Autoriteit Persoonsgegevens*) announced in August 2018 that the Dutch Chamber of Commerce (*KvK*), responsible for maintaining the Commercial Register, may even violate European data protection laws by providing advertisers access to personal data from the register.[129]

C. Findings

Overall, the legislator seems to make little effort to set out the purpose(s) of a particular register and what considerations inform the decision to fashion access in a certain way. Both in the relevant regulations and in the public record, the purpose of registers tends to be described very briefly and in general terms. The land registry is a clear example. The relevant act states that the purpose of this register is to promote legal certainty regarding registered real property and to support and promote economic activities.[130] While it may be impossible to provide all specific purposes, this general description for the land registry could be considered the other extreme.[131] A lack of specific purposes means that it is difficult to assess what processing operations are compatible with the legal basis.[132]

[125] *Kamerstukken* II 1982–83, 16143, nr 9 (Note on the final report Trade Register Act Amendment), 2.
[126] *Handelsregisterwet*, Stb 1996, 181.
[127] *Kamerstukken* II 2005–06 (n 76).
[128] Ibid.
[129] Joost Schellevis and Kysia Hekster, 'Privacywaakhond in Actie Tegen Datadelen Kamer van Koophandel | NOS' (*NOS*, 17 April 2018). Available at: https://nos.nl(last accessed 17 August 2019).
[130] Art 2a Land Registry Act (Kadasterwet).
[131] Berlee (n 38) 848.
[132] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203) 2013, 54.

Also noteworthy is the fact that the published legislative record (ie legislative proposals and explanatory memoranda, reports of parliamentary debates in both houses of parliament, outcome of public consultations and official reviews of registers) hardly ever testifies to a considered balancing of interests between the interests served by disclosure and countervailing privacy and data protection interests. It may not come as a surprise that on the issue of effectiveness of registers – do they achieve the public interest purposes they are meant to serve – few actual assessments seem to take place. As we have seen, where effectiveness has been reviewed, the outcome tends to be disappointing. Evaluations of the health care providers' register shows that patients hardly ever use it in their choice for a professional.[133] We elaborate on possible reasons for such outcomes below.

The absence of a substantive balance of interests in public legislative record is, in part, due to the long legal history of some public registers. Public registers have been in existence since as early as the sixteenth century.[134] Some public registers currently in existence have preceded more modern interpretations of privacy and data protection discussed in Section III. These include the application of Article 8 ECHR in the context of personal data;[135] the implementation of the Personal Data Protection Directive in the Dutch Data Protection Act in 2001;[136] and the CJEU's 2010 decision in *Volker und Markus Schecke and Eifert* that a disclosure of personal data should be preceded by a balance of interests.[137] Prior to the creation of EU data protection laws, the Dutch Persons Registration Act of 1989 (*Wet Persoonsregistratie*) also categorically excluded public registers from its scope without providing a balance of interests in this regard.[138]

Old registers, therefore, often lack extensive discussions on privacy and data protection. These should still comply with modern EU data protection laws. This has also been recognised by the Dutch legislator: during the implementation of the Data Protection Directive 95/46/EC, some purpose specifications were introduced for some – but not all – public registers already in existence.[139] The implementation would have been a great opportunity to show transparency about the proportionality of these registers. However, this did not happen. Neither did this occur during the entry into force of the CFREU or the implementation of the GDPR. As such, a broader review of the older registers may be expedient to assess compliance with current privacy and data protection standards. This may be even more important in view of the risks posed by the combined use of public registers

[133] Friele and others (n 104) 35.
[134] Berlee (n 3) 214–216.
[135] *Leander v Sweden*, judgment of 26 March 1987, Series A no 116, p 23.
[136] Entry into force of the Dutch Personal Data Protection Act, Stb 2001, 337.
[137] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, para 85.
[138] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet Persoonsregistratie*), 18; Art 2(2) Persons Registration Act.
[139] Act amending provisions related to the processing of personal data, Stb 2001, 180.

or public registers and other public information. We found hardly any discussion about the risk the combined use of public registers might impose on privacy and data protection.

V. Conclusions

The empirical analysis of Dutch public registers and the relevant legislative records indicates there is a persistent lack of attention for the question whether the objectives pursued by public registers justify the potential privacy harm. Also, government does not seem to assess whether public registers are actually effective instruments, whereas practice suggests they may not be.[140] What is more, to the extent that policy makers do visibly assess the effectiveness, the focus is on one particular register, not on the broader effects it may have because of what it adds to the existing pools of data. Broad empirical analyses of the kind done here, enable us identify trends and potential privacy problems. In a nutshell, the trend is towards more public registers and more online publication. The problems are that insufficient attention is paid to privacy concerns and to the systemic effects of increased availability of public register data. A key requirement in both EU data protection law and fundamental right to privacy (Article 8 ECHR) is proportionality. A public register, in its existence, design and operation, must be necessary (which also implies that it be effective) to achieve its legitimate purpose and not be more intrusive than necessary.

The number of registers that disclose information on citizens (whether in professional roles or not) is substantial and growing. Typically, they can be consulted online. These registers seek to balance information asymmetries on the market, promote trade and legal certainty with respect to (commercial) transactions.[141] However, it is unclear whether they are effective instruments in the pursuit of such goals. Yet new registers are constantly being introduced.

This is all the more worrisome since our research shows what can only be called a persistent lack of reflection by policy and lawmakers on the privacy risks posed by public registers. What justifies the level of 'publicness' of public registers is seldom well argued in the legislative record. The existence of older registers is used to justify the appropriateness and proportionality of new ones,[142] without the older registers themselves having been properly assessed on privacy and data

[140] Archon Fung, Mary Graham and David Weil, *Full Disclosure: Perils and Promise of Transparency* (Cambridge University Press, 2007) 40; Van Rein, Verwiel and Van Zoggel (n 82); Eshuis and Dijkhoff (n 79).

[141] Paul Frissen, *Het Geheim van de Laatste Staat Kritiek van de Transparantie* (Boom uitgevers 2016) 131–137; Fung, Graham and Weil (n 140) 5 and 40.

[142] College Bescherming Persoonsgegevens, 'Advies Voorstel Lerarenregister' (2015).

protection interests. Some ad hoc interventions based on incidents do occur.[143] It may, therefore, be good policy to regularly assess the compliance of these older registers with current privacy and data protection standards. How they contribute to potential adverse effects of having a network of growing number of online registers is also an issue to consider.

The use of (technological) security measures and access restrictions can obviously mitigate privacy risks. Such restrictions may limit bulk downloads or API limiting the uses that can be made of data. Our focus was not on such modalities of access. We would note, however, that the official records suggest that lawmakers generally pay little attention to these aspects. Shortcomings on the political level may trickle down into the actual design of a public register. This is not to say that government bodies tasked with designing and operating registers do not consider privacy issues in access design at all; but if and how this happens is not transparent.

The consistent use and publication of Privacy Impact Assessments (PIAs) can improve matters. Dutch central government has decided to run PIAs in all instances where a policy is developed, or a regulation proposed, that involves the processing of personal data. This can help improve design choices (what data to include in a register, how to make it available to the public). It also makes it easier to do ex-post evaluations. PIAs are, however, not necessarily published and the GDPR does not require them to be. Routine publication would be one way to stimulate that careful assessment of privacy implications is made, and to enable public scrutiny.[144] Research on these combined PIAs could also be valuable in identifying systemic risks.

Although the empirical work focused on Dutch public registers, it has broader implications. Public registers increasingly result from EU legislation. Furthermore, EU open government and open data policies, and global initiatives like the Open Government Partnership seek to increase the availability of existing public sector data resources for commercial and non-commercial use in the private sector.[145] Awareness is growing that the vast majority of data sets held by governments contain personally identifiable information, and that on various levels, data protection law is at odds with the notion that data should be 'shared' freely. The increased availability of non-personal, public sector data eventually becomes personal data if it can be linked with an expanding amount of public registers containing personal data (and also private sector sources), adding to the exposure of citizens.

[143] Eg when it became clear that persons who are threatened by, eg, former spouses, disgruntled employees or random stalkers can easily be traced by perpetrators on the basis of information from the Land Registry, the Dutch Government announced measures, Rijksoverheid, 'Informatie over Bedreigde Personen Niet Langer in Kadaster' 29 (2018).

[144] Ausloos (n 17).

[145] European Commission, 'European Legislation on the Re-Use of Public Sector Information | Digital Single Market' (2019). Available at: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information (last accessed 17 February 2019); Open Government Partnership, 'About OGP'. Available at: www.opengovpartnership.org/about/about-ogp (last accessed 19 February 2019).

References

Literature

Article 29 Working Party, 'Opinion 01/2012 on the Definition of Consent' (2011) WP 187.
——, 'Opinion 03/2013 on Purpose Limitation' (2013) WP 203.
——, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211.
——, 'Opinion 8/2014 on the Notion of Legitimate Interests of the Data Controller' (2014) WP 217.
——, 'Guidelines on Transparency under Regulation 2016/679' (2016) WP 260.
——, 'Opinion 02/2016 on the Publication of Personal Data for Transparency Purposes in the Public Sector' (2016) WP 239.
Ausloos, J 'Giving Meaning to Lawfulness under the GDPR – CITIP Blog' (2017). Available at: www.law.kuleuven.be/citip/blog/2761-2/ (last accessed 17 February 2019).
Bagger Tranberg, C 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 *International Data Privacy Law* 239.
Berlee, A 'Volledige Openbaarheid : Het Doel Voorbij' (2017) 2017 *WPNR* 844.
——, *Access to Personal Data in Public Land Registers, Balancing Publicity of Property Rights with the Rights to Privacy and Data Protection* (Eleven International Publishing, 2018).
'Bijbaan Voor de Burgemeester' *Brabants Dagblad* (2017).
'Burgemeester Wikt, Weegt En Zegt Die Ene Bijbaan Op' *Brabants Dagblad* (16 November 2017).
CBP, 'Actieve Openbaarmaking En Eerbiediging van de Persoonlijke Levenssfeer' (2009).
College Bescherming Persoonsgegevens, 'Publicatievan Persoonsgegevens Op Internet' (2007).
Eshuis, RJJ and Dijkhoff, N, 'Nevenfuncties Zittende Magistratuur' (2000) 185.
European Commission, 'European Legislation on the Re-Use of Public Sector Information | Digital Single Market' (2019). Available at: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information (last accessed 17 February 2019).
European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Data Protection Law* (2014).
Friele, R et al, 'Zorgverleners En Burgers over Het Openbaar Maken van Door de Tuchtrechter Opgelegde Berispingen En Geldboetes'. Available at: www.nivel.nl/sites/default/files/bestanden/Tuchtrecht_impact_van_openbaar_making.pdf (last accessed 19 February 2019).
Frissen, P *Het Geheim van de Laatste Staat Kritiek van de Transparantie* (Boom uitgevers, 2016).
Fung, A, Graham, M and Weil, D, *Full Disclosure: Perils and Promise of Transparency* (Cambridge University Press, 2007).
Gerards J, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466.
Hulst, EH, 'Naming En Shaming van Artsen Die Tuchtrechtelijk Zijn Veroordeeld' (2017) 2017 *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 1.
Kloek-tromp, IJ, 'Kadaster En Privacy in Praktijk' (2017) *WPNR* 853–858.
Lind, A-S and Strand, M, 'A New Proportionality Test for Fundamental Rights?' (2011) 7 *European Policy Analysis* 1–11.

McDonagh M, 'The Protection of Personal Information in Public Registers: The Case of Urban Planning Information in Ireland' (2009) 18 *Information & Communications Technology Law* 19.

Ministry of the Interior and Kingdom Relations, 'Model Gegevensbeschermings-Effectbeoordeling Rijksdienst (PIA)' (2017).

NORA, 'NORA Online'. Available at: www.noraonline.nl (last accessed 19 February 2019).

Oostveen, M, *Protecting Individuals Against the Negative Impact of Big Data: Potential and Limitations of the Privacy and Data Protection Law Approach* (Wolters Kluwer, 2018).

Partnership OG, 'About OGP'. Available at: www.opengovpartnership.org/about/about-ogp (last accessed 19 February 2019).

Rijksoverheid, 'Informatie over Bedreigde Personen Niet Langer in Kadaster' *29* (2018).

Schellevis, J, 'Gegevens KvK-Inschrijvingen Gebruikt Voor Reclames Op Facebook | NOS' *NOS* (18 April 2018).

Schellevis, J and Hekster, K, 'Privacywaakhond in Actie Tegen Datadelen Kamer van Koophandel | NOS' (*NOS*, 17 April 2018). Available at: https://nos.nl (last accessed 17 August 2018).

Sijmons, JG et al., 'Tweede Evaluatie Wet Op de Beroepen in de Individuele Gezondheidszorg' (2014) 4 *Tijdschrift voor Gezondheidsrecht* 264–281.

Tomesen WBM, 'Advies Voorstel Lerarenregister' (2015).

Van der Hoorn, S, 'Gegevensopstraat.Nl'. Available at: www.gegevensopstraat.nl/ (last accessed 17 August 2018).

Van Eechoud, M and Prins, C, 'Directive on Public Sector Information Re-Use' in Serge Gijrath and others (eds), *Concise European Data Protection Law, E-commerce and IT Law* (Kluwer Law International, 2018).

Van Rein, E, Verwiel, E and Van Zoggel, M, 'Het College Klust Bij' [2017] *De groene Amsterdammer*.

Versmissen. JAG and De Heij ACM, 'Elektronische Overheid En Privacy' (Den Haag, College bescherming persoonsgegevens, 2002).

'Wat Is Persoonsregistratie? | Persoonsregistratie | Arboportaal'. Available at: www.arboportaal.nl/onderwerpen/persoonsregistratie/wat-is (last accessed 18 August 2018).

Winter, H, Geertsema, B and Krol, E, 'Evaluatie LEC-SVH' Available at: www.dhwinspecteur.nl/wp-content/uploads/2016/10/evaluatie-lec-svh.pdf (last accessed 18 August 2018).

Zuiderveen-Borgesius, FJ, *Improving Privacy Protection in the Area of Behavioural Targeting* (Wolters Kluwer Business 2015).

Zuiderveen Borgesius, F, Van Eechoud, M and Gray, J, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30 *Berkeley Technology Law Journal* 2073.

Case law

European Court of Justice

Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18.

Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50.

Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, [2014] 3 CMLR 44.

Joined Cases 509/09 and C-161/10 *eDate Advertising ao* ECLI:EU:C:2011:685, [2011] ECR I-10269.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063.
Case C-524/06 *Huber* ECLI:EU:C:2008:724, [2008] ECR I-09705.

European Court of Human Rights

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [GC], no 931/13, ECHR 2017 (extracts).
Leander v Sweden, judgment of 26 March 1987, Series A no 116, p 23.