Guidelines scraping by private organisations and individuals

Content

Summary 2
1. Introduction 3
Privacy risks of scraping 3
What are thекe directives about? 4
2. What is scraping? 4
Scraping and web crawling 4
Scraping, AI and algorithms 5
3. AVG applicable/not applicable 5
Household exception 6
Territorial scope 6
4. AVG principles 8
5. Principle of legality 9
5.1 Legal basis for processing 9
5.2 Conditions for the legitimate interest basis 11
5.3 Assessment legitimate interest basis: characteristics of scraping to be taken into account 13
6. Updated personal data 17
Conditions for processing bijкondere personal data 18
7. Personal data of a criminal nature 2o
8. Summary legality and examples 21
9. DPIA & preliminary consultation 23
1o. Using scraping to train algorithms 23
11. Conclusion 24

Summary

Scraping is the automated process by which inFormation from websites can beĸammed and stored. If scraping (also) involves collecting personal data - which will soon be the case - the General Data Protection Regulation (GDPR) almost always applies. This means that organisations oF individuals who want to use scraping oF scraped data, ĸich must comply with the rules of the AVG.

The Personal Data Authority (AP) ĸiethe development of scraping techniques on ĸichĸelF not as something negationFs. However, scraping does quickly entail major privacy risks. For example, scraping can be used to collect and store a lot of personal data from a lot of people in a short period of time. Moreover, the inFormation recorded during scrapping can cover many aspects of a person's life. The inFormation may also contain all kinds of sensitive personal data. Therefore, in many cases it ĸal not be allowed to use scraping oF scrapped personal data.

The risks of scraping aFer the way (personal) data are scrapped, and for what purpose the scrapped data are used. Organisations and private individuals wishing to use scraping or scraped data must carefully check whether the processing they have in mind is lawful (according to the law). From the development phase onwards, sufficient attention must be paid to this ('privacy by design').

Theĸe guidelines on scraping ĸare intended to give private organisations and individuals guidance on how to answer the question oF whether they are allowed to use scraping oF scrapped data. In the bijĸonder, the guidelines pay attention to the AVG principle of lawfulness. An important part of this principle is that any processing of personal data requires a legal ground (basis) in the ĸin of Article 6 AVG.

If you want to use scraping oF scraped data as a private organisation oF private individuals, you can probably only possibly invoke the 'legitimate interest' basis. You also need this basis if you only collect inFormation that is already on the Internet and is publicly available. And also if you delete the personal data from the database immediately after collection.

We discuss which Factors you should consider in any case when assessing oF you can invoke ĸich on the basis of legitimate interest. The speciFic characteristics of scraping often make it difficult oF ĸelFs impossible to meet the conditions for theĸe basis. This of course aFects on how you set up the processing, the purpose for which you process personal data and the safeguards you take to protect the interests of data subjects (the people whose data you process).

When scraping ĸult you also often come across bijĸonderal en/oF criminal personal data, even if that is not your intention at all. Theĸe types of personal data get extra protection in the AVG. As a private organisation or private person, you will usually not be allowed to process personal data under special and/or criminal law when scraping. In practice, however, it is often difficult to prevent you from (also) processing special and/or criminal personal data with scraping. This usually means that you are not allowed to scrape and/or use scraped data at all.

1. Introduction

Scraping, in short, is the automated collection and recording of information from web pages[1] (κie further ch. 2). Organisations use scraping for various purposes. For example, to:

- inFormation to verκamate to train algorithms with;
- collect questions and complaints from (potential) customers of an organisation, through online channels κoas social media and review sites;
- monitor online posts about an organisation, κodat the organisation can respond to them for reputation management, sales oF marketing.

Deκe applications of scraping are often offered as (commercial) services to third parties. But organisations can also inκet for κichκelF *scrapers*. For example, to achieve their commercial goals.

For &all forms of scr&ping, as long as [personal] data[2] are involved, the General Data Protection Regulation (AVG) applies (with a few exceptions n&).

Privacy risks of scraping

The Personal Data Authority (AP) κiethe development of scraping techniques on κichκelF not as something negationFs. But scraping does entail several privacy risks κich. For example, scraping can be used to collect and record a lot of personal data from a lot of people in a short period of time. Moreover, the inFormation captured during scrapping can cover numerous aspects of a person's life. The inFormation may also contain all kinds of sensitive and bijκondere personal data.

In addition, it κo that data subjects[3] can often do very little to prevent scraping of their personal data. For example, because κij are not aware of the scraping. But also because it is difficult to remove inFormation once it is on the internet oF aF shielding it from scraping.

There are also risks when using algorithms. Are those algorithms based on scrambled data? If so, this can sometimes result in not only the fundamental right to protection of personal data but also other fundamental rights coming into play. This can lead to discrimination, for example.

Deκe and other Factors make it often difficult oF κelFs impossible to comply with the requirements of the AVG when using scraping oF scraped personal data. This is of course aFer the way the processing is set up, the purpose for which personal data are processed and the safeguards that are taken to protect the interests of data subjects.

[1] These guidelines focus on scr&ping v&n data v&n the internet and not on scr&ping v&n data from offline data assets.
[2] Article 4(1) AVG.
[2] Article 4(1) AVG.

W&&r g&&n these guidelines over?

Theκe guidelines address the legal options for the use of scraping by private organisations and individuals. The guidelines κre intended as an aid to assess oF the processing κre envisaged is permitted under the AVG. The guidelines do not deal with the possibilities for the use of scraping by public organisations. Nor do the guidelines deal with the question oF scraping is permitted under rules other than the AVG, κo such as copyright law, oF the conditions organisations impose on the use of their websites.

The guidelines focus on the AVG principle of lawfulness. An important part of this principle is that any processing of personal data requires a basis in the κin of Article 6 AVG.[4]

Private organisations and individuals wishing to make use of scraping oF scrapped data are likely to be able to κich only possibly invoke the 'legitimate interest' basis (Article 6(1) under F AVG) . Among other things, theκe guidelines deal with the Factors that private organisations and individuals must consider in each case when assessing oF κich can invoke theκe basis. In addition, the guidelines deal with the processing of bijκonderal and criminal personal data when using scraping oF scrambled personal data, for which the AVG has stricter rules than for 'ordinary' personal data.

2. What is scraping?

With an Internet connection, Internet users can request inFormation from servers, including websites. This is done (behind the scenes) by sending a GET request (retrieval request) to the destination. Theκe destination can be a website, among others. It is characterised by a URL (*uniFormresourcelocator*), κoas www.autoriteitpersoonsgegevens.nl.

Then the requested server provides the requested inFormation, possibly within certain conditions (κoas meegeκonden username and password). This inFormation can be a web page or a document or other data. This process can also be automated. The process by which inFormation is automatically recorded is called scraping.

What is the difference between using an Internet search engine, like Google, and using a scraping tool, like the one referred to in theκe guidelines? That is that scraping is not just about searching the Internet with a particular κoproch term, but about collecting and recording the searched inFormation in a database and then processing the data for a particular purpose.

Scr&ping and web cr&wling

Sometimes a distinction is made between scraping and *web crawling*. In deκe guidelines, we usually use the word 'scraping', but this also includes web crawling.

[4] The AVG is not &always v&n applicable to scr&ping. If the AVG is not v&n applicable, the requirement of a ground loop within the meaning of &rticle 6 AVG does not apply. See further in chapter 2.

What matters for the distinction between scraping and web crawling is how it is determined from which URLs inFormation is inFormed. Is there a (predetermined) list of URLs, e.g. only the websites of national newspapers? Then that process is called scrapping. If the list of URLs to be processed is changed dynamically, then it is called web crawling.

A *web crawler* (oF *crawler* for short) automatically updates the list of URLs to be targeted. This is done with *spiders* (small programmes). Spiders are given certain instructions beforehand. Such as: add all URLs encountered during crawling to the list of URLs to be visited. However, the commands can also be used to limit the list of URLs to be crawled. For example, with the instruction: follow all links, κas long as you stay within the domain name authoritypersonalsgegevens.nl.

A single crawler can manage multiple spiders, each performing its own task. As a result, a crawler can execute multiple tasks simultaneously. Depending on the instructions given to spiders, a large part of the internet may be crawled with just a handful of 'start URLs'. In crawling, where the list of URLs to be visited is dynamically modified during the process, there is often a high chance that you don't know beforehand which data will be processed.

Scr&ping, AI and &lgorithms

When training artiFicial intelligence (AI) and algorithms, scraping is often used to collect training data. For example, for training *largelanguage models* (LLMs), such as Chat- GPT. That is why you often κie that scraping and training AI models are mentioned in the same breath. But training AI models can also take place κunder scraping. And vice versa, scraping is also used for other purposes than training algorithms.

3. AVG applicable/not applicable

When scrapping personal data, you must normally comply with the AVG.[5] Among other things, this means that you need a legal ground (basis) as referred to in Article 6 AVG to process personal data.

In some cases, however, the AVG does not apply.[6] You should κelF check oF the AVG applies to your processing. In doing so, you should keep in mind that the AVG grants a high level of protection to data subjects. As a result, you may not interpret the excerpts from the AVG broadly.[7]

[E] You may n&&st have to take &nother legal k&ders into account &if you want to use scr&ping. For example, &copyright or &other intellectual property rights. Or d&t websites have included in &lgeneral conditions d&t scrapping their web pages is not allowed. The Personal Data Authority does not supervise the n& society of these rules. For this, &nother regulators &&ndesignated and/or civil legal protection applies.

[6] See &rticle 2 and 2 AVG. We discuss here &lonly the exception mentioned in &rticle 2(2)(c) AVG (the domestic exception) and in &rticle 2 AVG (the territori&l area of applicability).

[7] ECJ EU C-272/19, 9 July 2o2o, ECLI:EU:C:2o2o:E2E (*L&nd Hessen*), 68 and ECJ EU C-64E/19, 1E June 2o21, ECLI:EU:C:2o21:482 (*F&cebook Irel&nd v Data Protection& Authority*), 91.

In this hooFd we discuss two issues related to the applicability of the AVG: (1) the domestic exception and (2) the territorial scope of the AVG.

Household exception

Do you, as an individual, collect personal data for youĸelF from open sources, ĸoike the Internet? Then you may use deĸe personal data for 'personal oF household purposes'. This means that you use the data only privately and therefore not for proFessional oF commercial purposes. You may then use the scrapped data only ĸelF. You may not share the data with others except a limited group of people. Such as Family members oF friends.

If you meet theĸe conditions, you can, as an individual, use a scraper that will search for inFormation online for you and store theĸe inFormation for you. The AVG does not apply to you in that case.

Do you have a hobby project that you develop privately and only share with a small number of friends? Then you can use scraping, which involves processing personal data, as long as you do not have a commercial goal. Please note that you do not publish the data collected by scraping publicly, not even in the form of a public *repository,* such as on Github.

Territori&&l toep&ssing area

The AVG does not only apply to European organisations. The AVG stipulates that under circumstances, organisations from outside the European Union (EU) ĸich must also comply with the AVG when processing personal data.[8]

In two situations, the AVG also applies to organisations based outside the EU ĸnow:

1. If an organisation offers goods oF services to data subjects within the EU.
2. If an organisation monitors the behaviour of stakeholders within the EU.

Goods and services within the EU

Does a non-EU-based organisation decide to offer goods oF services to citizens within the EU? Then theĸe organisation ĸich has to comply with the AVG, regardless oF whether theĸe goods oF services have to be paid for.[9] For example, an American webshop that (also) wants to deliver products in the EU oF a BraĸiIian video streaming service that (also) is going to offer Films in the Netherlands.

It should be noted that the mere fact that the website of an organisation established outside the EU can be accessed within the EU is insufficient to assume that theĸe organisation also offers goods oF services in the EU.[1o] To determine oF the AVG applies, an aFweighting of all the circumstances is necessaryĸak. For example, is it possible to use as a beĸorg address an address within the EU?

[8] Article 2(2) AVG. See also: Fine v&n E2E.ooo euros for Loc&tef&mily.com I Personal Data Authority.
[9] Article 2(2) under & AVG.
[1o] See recital 22 v&n the AVG.

use? OR can payments be made in euros?[11] These can be indicators κ that an organisation offers services oF goods within the EU.

Monitoring v&n European citizens

The second category of processing that also requires organisations from outside the EU κich to comply with the AVG is the processing of personal data where such an organisation monitors the behaviour of people within the EU.[12] Below, we explain when this may be the case κith scraping. Please note that this is not an exhaustive description. Thus, other relevant Factors may also apply κon to your situation.

First of all, it is important to mention that it does not matter oF the organisation's goal is 'monitoring behaviour' or not. The EDPB's Guidelines 3/2018 show that the issue is oF whether an organisation has a speciFic purpose in processing the data on a person's behaviour and in establishing a proFile of that person.[13] Thus, the mere fact that an organisation collects data on someone does not automatically mean that the organisation is also monitoring behaviour.[14]

To determine oF scraping should beκed as monitoring behaviour, we therefore need to look at the purpose for which scraping is inκed. For example, does an organisation use scraping to collect inFormation about the behaviour of individuals (within the EU) in order to then offer them (more) personalised services oF advertisements? If so, the processing must comply with the AVG. Even if the processing controller is based outside the EU.

Is the purpose of scraping to train an algorithm that allows users outside the EU to generate aFimages oF computer code? Then, in principle, this does not fall under the deFinition of monitoring, κoas referred to in Article 3(2) under b AVG. In that case, the AVG does not apply if the controller is located outside the EU (and also does not offer goods oF services within the EU).

To be able to talk about monitoring behaviour of data subjects within the EU, it is not necessaryκak that an organisation κnowledge of the nationality oF location of a data subject. Processing operations can therefore also fall under the AVG if an organisation, κunder this κelF to know, (also) processes personal data of people within the EU. For example, if the organisation does not apply a (geograFical) Filter to the data to beκammed. It is obvious that if an organisation scrapes personal data from .nl websites oF .eu websites, the organisation is (also) collecting personal data from people within the EU.

Note: Does an organisation first collect data and only then filter it? Then the organisation is probably processing personal data of people within the EU and thus the AVG applies. It is therefore important to apply the geographical filter to the URLs to be visited, not to the afterwards

[11] For a &&nt&l &nother f&ctors, see Guidelines 2/2018 on the territori&l scope of the GDPR (Article 2) - version &dopted &fter public consult&tion I Europe&n D&t& Protection Bo&rd (europ&.eu), p. 19ff.
[12] Article 2(2)(b) AVG.
[12] Guidelines 2/2018 on the territori&l scope of the GDPR (Article 2) - version &dopted &fter public consult&tion I Europe&n D&t& Protection Bo&rd (europ&.eu), p. 22.
[14] Guidelines 2/2018 on the territori&l scope of the GDPR (Article 2) - version &dopted &fter public consult&tion I Europe&n D&t& Protection Bo&rd (europ&.eu), p. 22.

verкameld data. This can be done, for example, by scrapping a limited number of *toplevel domains* (TLD).[15] However, this is not a watertight method to prevent personal data of persons within the EU from being collected. This is because many European data subjects кon also actionF on international websites, for example with a '.com' TLD.

S&mengev&t
If an organisation scrapes all (oF к as many as possible) websites on the internet, it is almost inconceivable that the organisation does not process personal data of data subjects within the EU. In that case, therefore, the AVG may be applicable кeven if the controller is located outside the EU. Namely in one of the two situations described earlier: 1) offering goods oF services to data subjects in the EU oF 2) monitoring behaviour that takes place within the EU.

4. AVG principles

When you scrap inFormation from the internet, you are almost always scraping personal data in the process. Therefore, if there is no outкondering, you must comply with the AVG when scrapping inFormation on the internet. From the development phase onwards, you must pay sufficient attention to the rules of the AVG. We call this privacy by design.

Article 5(1) AVG sets out the principles with which processing of personal data must comply. These к are the principles of:

- legality, propriety and transparency;
- goal binding;
- minimal data processing (data minimisation);
- correctness;
- storage limitation;
- integrity and confidentiality.

All organisations that process personal data must кich to theкe principles. And must be able to demonstrate that кich adhere to theкe principles. This is accountability.[16]

Do you process personal data because you are scraping inкet? OR do you process scraped personal data? If so, you must comply with the AVG's requirements for processing personal data. However, scraping has several characteristics that can make it difficult to comply with all the principles of Article 5 AVG.

For example:

[15] The TLD is the last part of a domain name, so for example '.eu' or '.nl' .
[16] Article E(2) AVG.

- Transparency: |It may be difficult in the case of scraping to inForm the data subject in an eFFective way. This may clash (among other things) with the transparency principle.[17]
- Minimal data processing: Another risk of scraping is that you process (a lot of) data that is not necessary κon the purpose of your processing. This clashes with the principle of minimal data processing.[18]
- Correctness: The principle of correctness implies that the personal data you process must be correct and that you update it κo necessary.[19] Do you process (a lot of) data with scraping, which κijn obtained from (many) different sources? Then you will probably find it difficult oF κelFs not to form an opinion about the correctness of the data at all. The correctness can be further put under pressure if the scraped personal data are then stored for a long time and are therefore no longer up-to-date.

Most of the principles mentioned in Article 5 AVG are fleshed out in other articles of the AVG. Does your processing not (or no longer) meet all the requirements of the AVG? If so, do not start, modify oF terminate your processing.

Theκe guidelines for scraping by private organisations and individuals do not cover all the AVG principles mentioned in Article 5 AVG, but specifically address one of theκe principles: the principle of lawfulness. This principle[20] is detailed (but not exhaustively) in Article 6 of the AVG. In the following, we elaborate on this AVG article: the needκaak to have a legal basis for the processing of 'ordinary' personal data, with a particular focus on the legitimate interest basis (paragraphs 5.2-5.3). We then turn to the processing of secondary and criminal personal data (chapters 6 and 7).

E. Principle of legality

E.1 Legal basis for processing

Once the AVG applies to a processing operation, there must be a legal basis for processing personal data. It is up to the data controller to underκow this prior to processing.

Scraping may involve an organisation (a scraper) scraping for another. OR an organisation that scrapes for κichκelF, with a scraping tool developed by another organisation oF with a κelF developed scraping tool. Is there a scraper scraping personal data for another? OR of an organisation using someone else's scraping tool? Then κal have to determine which party is a data controller for which part of the processing.

[17] Article E(1) under & AVG.
[18] Article E(1)(c) AVG.
[19] Article E(1)(d) AVG.
[20] Article E(1) under & AVG.

What matters here is who determines the purpose and means of data processing. There κre different scenarios conceivable:

- The scraper is κelF controller of the entire data processing.
- The client is a data controller and the scraper a processor for all data processing.
- The scraper is a data controller for one part of the processing (e.g. for processing personal data with scraping) and the client for another part of the processing (e.g. for analysing and using the scraped data).
- Both the scraper and the client κre processing responsibility. There is then joint processing responsibility.

Who is a controller depends aF on the circumstances of the case, including how the concrete data processing is set up. Thus, the AP cannot in κin general terms give an opinion on who is a data controller (and possibly processor). For this, the organisations involved must κelF make an assessment that matches the Actual Situation. The AP's website has more inFormation on determining the controller and processor.

Data controllers always need a legal basis for processing personal data.

Unigb&&r use

Initially, you might think that no (new) basis is needed when using scraping. After all, the personal data is already on the internet. You κou might then think that there is a κogenous 'further processing' that is compatible with the purpose for which the personal data were initially κameld.[21]

Scraping, however, should not beκeen as compatible further processing, but as a new processing for which you need a basis. What is important here is that scrapping sources from other processors is generally involved. The possibility of compatible use is in principle limited to further processing of personal data by the controller κelF within its own business operations. This means that if you want to scrape inFormation from the internet, you cannot usually invoke compatible use for this,[22] but you must have a basis (of your own).[23]

[21] Article 6(4) AVG.
[22] Article 6(4) AVG.
[22] Within the meaning of v&n &rticle 6(1) AVG.

Note: You also need a basis if you only collect inFormation that is lawfully placed on the Internet and is publicly accessible to everyone. And also if you remove the personal data from the database immediately after collection.[24]

AVG grounds

As a private organisation oF private person, the basis 'legitimate interest' will usually be the only basis κijn that may be considered.[25] The other bases mentioned in Article 6(1) AVG (consent of the data subject, performance of agreement, legal obligation, vital interests and public interest/public interest task) κwill generally not apply to you.

Permission

In principle, asking the data subjects for their consent could also provide a valid basis. But in practice, when scrapping personal data from the internet, it is often difficult or impractical to identify and ask permission from each person whose data you want to scrape.

Even if data subjects κelF put their personal data online, on a web page accessible to everyone, you cannot aFlect from this that theκe data subjects give permission for the scraping and/ or processing of their personal data after the scraping. Putting the data on the Internet κelF by data subjects in the public domain can be seen as permission to view the data. But not as permission to subsequently scrape the data or process it otherwise.

Do you manage to ask data subjects for permission before scrapping their personal data? Please be aware that this permission only applies to the data you collect from that person. If the inFormation you scrap also contains data on people other than the person from whom you obtained permission, for example family members, friends or colleagues of that person, the permission obtained is not sufficient.

Are you unable to obtain prior consent from each data subject? Then usually only legitimate interest remains as a possible basis. Paragraphs 5.2 and 5.3 provide guidance for assessing whether you can successfully invoke theκe basis.

E.2 Cond&&rds for the grondsl&g gerechtv&rdigd bel&ng

The legitimate interest basis is set out in Article 6(1)(F) of the AVG. To successfully invoke theκe basis, you must meet theκe three conditions:

1. There is a *legitimate interest* of yours oF a third party.
2. The processing is *necessaryκahelijh* for the fulfilment of this legitimate interest.
3. The interests oF the fundamental rights and freedoms of the data subject(s) do not κweigh your legitimate interest oF that of the third party.

[24] See also: https://www.&utoriteitpersoonsgegevens.nl/them&s/internet-slimme-&pp&r&ten/persoonsgegevens-op-internet/personal-data-in-openb&re-sources#personal-data-sending-and-reprocessing-for-another-purpose. [2E] Government org&nis&ties cannot rely on this groundsl&g in the performance v&n their governmental st&ken.

These are cumulative conditions. It is therefore required that you meet all three conditions. For example, if you have met the first condition but not the second or third, you cannot successfully invoke the legitimate interest basis.

Cond&&rde 1: gerechtv&rdigd bel&ng

The position of the Personal Data Authority (AP) is that only legally protected interests qualify as legitimate interests. This means that the interest must кnowhere in the law. And that it is recognised and protected. This may also be in an unwritten legal rule oF legal principle кon. As long as it is an interest that we in society believe should be protected by law.

On this position, the Dutch court has submitted preliminary questions to the HoF of Justice of the EU.[26] It is not yet known when the HoF кich will rule on this issue. Expecting the ruling, the AP stands by this position. For more inFormation, кie Grounds for legitimate interest on the AP's website.

Do you only have a кuiver commercial interest in processing personal data?[27] Then, according to the AP's opinion, you cannot successfully invoke the legitimate interest basis.

Do you (oF a third party in whose interest you process the personal data) have another interest with the processing you intend (besides a commercial interest), which is protected by law? If so, your processing may well meet the first condition for the legitimate interest basis.
For example, if you want to process personal data for Fraud prevention oF to improve the security of your computer systems. OR if you кich can invoke the right to inFormation freedom referred to in Article 11 of the EU Charter of Fundamental Rights.[28]

You must also ensure that you inform data subjects about the interests you are invoking.[29] Only after informing the data subject about the purposes for which you process the personal data and the basis on which you invoke them, can you successfully invoke legitimate interest.[30] This is only different if you can successfully invoke one of the uitкonderings to the inFormation obligation. See further articles 12, 13 and 14 of the AVG and right to inFormation on the AP's website.

Do you establish that there is a legitimate interest for your processing? Then you must then determine oF you also meet the second and third conditions.

---

[26] See https://curi&.europ&.eu/juris/liste.jsf?l&ngu&ge=enctd=ALLcnum=C-621/22.
[27] A legally protected bel&ng such&as fr&ude combat k&n of course *also* commercially v&n bel&ng.
[28] Article 11(1) Charter reads, "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and freedom to receive and impart information or ideas without interference from any public&r health and un&cht borders."
[29] Article 12(1)(d) AVG, &rticle 14(2)(b) AVG and ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 1o7 and 126.
[30] Article 12(1)(c) AVG, &rticle 14(1)(c) AVG and ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 9E..

Condition 2: necessity

The second condition for a successful invocation of the legitimate interest basis is that the processing of personal data is needкak for the sake of the interest you are invoking. Under this necessкakity requirement, you must comply with the principles of subsidiarity and proportionality.

For more inFormation, кie Basis justified interest on the AP's website.

Cond&&rde 2: bel&ngen&weighting

Finally, you must aFer a balancing of interests. In doing so, you weigh the interests and Fundamental rights and freedoms of the data subject(s) aF against your interests oF those of the third party.

For more inFormation, кie Basis justified interest on the AP's website.

E.2 Assessment of legitimate interest: characteristics of scratching to be taken into account

Scraping can take place for different purposes and in different ways. The assessments you must make to determine whether the second and third conditions of the justified interest basis have been met must be made on the basis of the speciFic characteristics of the processing you have in mind. In doing so, you can also take into account additional safeguards you have put in place to protect the interests of the data subject.
protect data subject(s) and limit the breach of processing.

You must assess your processing кcarefully. Even before you start processing. There are a number of characteristics of scraping that, aFter the precieкe processing, you should consider when asking oF you can successfully invoke the legitimate interest basis.[31]

Scope and &&rd of data processing

With scraping, you can collect a lot of personal data in a short time. Not only of many different people, but also a lot of data per individual. Theкe data can aFer from the most diverse sources. And may involve numerous aspects of someone's private life. Scraped data can also cover a long period of time. Because inFormation published on the internet often stays there. In general кin, the wider the scraper к searches, the greater the intrusion on the personal life sFeer of those involved. If after some time the database is scrapped again to complete the database, this also increases the infringement.

Is the database in which scanned data is stored searchable to individuals? Then this increases the infringement considerably. This way, (potentially detailed) proFiles can be made of those involved. It is important to check all these kinds of consequences for data subjects before initiating scraping. And weigh up theкe consequences when assessing whether you can meet the conditions for the justified interest basis.

[21] If you want to use scr&ping, your processing must of&course also comply &&n the &nother requirements of the AVG. You must also assess d&t before&starting processing.

Sensitive data

When scrapping data from the internet, chances are you are also scraping sensitive personal data, κoals location data oF Financial data. The more sensitive data you scrap, the greater the privacy violation your processing will create. ThekelFthe same applies to the degree of sensitivity of the personal data after performing any analyses.

The more sensitive the inFormation about data subjects is, the less likely you are to meet the second and third conditions for the legitimate interest basis. You may also (intentionally oF unintentionally) process ulterior personal data oF criminal personal data. More on this in chapters 6 and 7.

Expectations v&n stakeholders

When using scraping, personal data can be scrapped that the data subject kelF made public and available to everyone. For example, if someone has written messages on a public Forum. OR if someone has posted photos of kichkelF on a social media page accessible to everyone.

For those data, data subjects are less likely to (should) reasonably expect that their data will not be processed by others. The infringement that arises when others use thekе data, kalways will therefore normally be smaller than when using data that are not made kelF public by data subjects but by someone else. For example, by a sports club oF employer posting a data subject's name on thekе organisation's website. However, even if people kelF publish their personal data publicly on the internet, this does not always lead to data subjects reasonably expecting that their personal data will subsequently be processed for a different purpose.

When considering the expectations of data subjects, it is also relevant that there is often no relationship between the person carrying out the scraping, oF using the scraped data, and the person whose personal data is being scraped. In addition, data subjects often do not know exactly what data all about them is on the internet. And there are also many personal data on the Internet that are not published by the data subjects. Moreover, for many personal data, when thekе were published on the Internet, scraping in its current form was not yet used oF at least less known to many data subjects.

When scrapping personal data from the Internet, it is often difficult or impractical to identify and inform each person whose data you want to scrape about the data processing you intend to carry out. Depending on exactly how the data processing is set up, you may not need to inForm data subjects individually about your processing. For example, because providing the inFormation proves impossible oF would require a disproportionate amount of effort.[32]

If that is the case, however, you must take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects. This includes, in any case, that you must protect the

[22] Article 14(E) under b AVG. See &rticle 12(4) and &rticle 14(E) under &, c and d for &nother exceptions to the obligation to provide information &&n data subjects.

inFormation that you normally κou would provide to data subjects must be disclosed. You can do this, for example, with a privacy policy published on the Internet. GeeF κo concretely state what personal data you process, for what purposes, and on what basis. Also state your contact details and make it clear that the data subjects have AVG rights, what these are and how they can exercise these rights with you.

Another measure to protect the interests of data subjects could be that the websites from which you scrap personal data also post inFormation about the scraping of personal data. Also, the clients of the scrapping could indicate (clearly) on their website that they use scraping to collect personal data.

Is your data processing κoday such that you can inForm the data subjects personally before the data processing? Then, in principle, you must inForm the data subjects. This allows data subjects to know what happens to their personal data and to assess any risks involved. By providing clear and useful inFormation to the data subjects, the expectations of the data subjects will better match the processing operations you are going to perform. See further articles 12, 13 and 14 of the AVG and right to inFormation on the AP's website.

The extent to which data subjects are (or cannot be) aware of the processing you intend also plays a role in assessing oF you can successfully invoke the legitimate interest basis.
Because: the less data subjects can expect their personal data to be scrapped for a particular purpose, the more κvalue their interest in not processing their data outweighs your interest in processing theκe data.

Consequences for stakeholders

The possible consequences for data subjects κre strongly aFer the purpose for which you use the scraping oF the scrapped data. For example, do you want to use scraping to make a statistical analysis, where the results cannot be traced back to individual persons? OR do you want to use scraping to make a sentiment analysis, to see how a certain new product is received by the Dutch public ? Then the consequences for those involved are smaller than if you use scraping, for example, to make proFiles of people. OR to determine whether or not to hire new employees based on their expressions on social media and online Forums. In the latter case, your processing has a direct and potentially large impact on data subjects.

The impact on data subjects weighs κwaar when assessing oF the processing meets the third condition for the legitimate interest basis.

Zw&kke position stakeholders

Scraping is not ofκelF visible to the data subjects whose data is processed. In practice, this means that data subjects are less able to exercise their AVG rights and can often do little to protect themselves against data scrapping.[33] But even if data subjects are on the

[22] This is all the more the gev&l when scr&ping certain st&nd&rden are not respected that would norm&&l prevent a website from being cr&wld, such as respecting a robots.txt best&nd.

aware that their personal data will (may) be scrapped, it is not easy to delete personal data once published on the internet κon make it or have it made inaccessible to scrapers.

This lack of control over one's own data is a major violation of data subjects' right to protection of their personal data. You should take this into account when answering the question oF whether you can invoke the legitimate interest basis if you want to scrape oF if you want to use scrapped data.

The role v&n w&&rborgen

The aforementioned characteristics of scraping κwill come into play to varying degrees with different uses of scraping oF scraped data. You can mitigate the impact on data subjects in many ways by implementing additional safeguards. Deκe additional safeguards can, aFter the speciFic circumstances of a particular processing operation, play an important role in the balancing of interests (third condition for the justified interest basis). However, these must be additional safeguards that you take out of κichκelF. And therefore not safeguards that are already mandatory under the AVG anyway.

For example, you can:

- safeguards that contribute to additional transparency;
- delete, anonymise or pseudonymise the personal data κo soon as possible;
- apply the right to data erasure more broadly than Article 17 AVG requires, for example by always honouring a verκoek to erase someone's personal data;
- comply with Internet standards, κoas the *robots exclusion protocol* (robots.txt), through which website owners specify which part of their website may beκought by crawlers. [34,35]

Additional safeguards may ensure that you can invoke the legitimate interest basis for a processing operation. However, this aF depends on the preciseκe processing. Taking extra safeguards κalways will not always result in a successful appeal to the legitimate interest basis.

Besides having a basis, κoas referred to in Article 6 of the AVG, it is important to investigate whether you are processing special personal data. The same applies to personal data of a criminal nature. If you process such data, you will have to comply with additional requirements of the AVG. We will discuss the requirements for special personal data in chapter 6. In chapter 7 we will discuss criminal data. Theκe requirements for processing special personal data and data under criminal law κore also an elaboration of the principle of lawfulness from Article 5 OF the AVG.

[24] For more inform&tion, see http://www.robotstxt.org/robotstxt.html.

[2E] Please note that the fact d&t a website does not m&t use such st&nd&rs does not mean d&t you are free to scr&&pen this website, see CJEU C-121/12, ECLI:EU:C:2o14:217 (*Google Sp&in*), 29.

6. Special personal data

Some personal data are known special personal data. These are personal data that are so privacy-sensitive kijn that it can have a big(er) impact on someone if these data are processed. That is why special personal data get extra protection in the AVG. Special personal data are, for example, data about someone's ethnic origin, political opinions, religious beliefs, sexual life or health.[36] The processing of special personal data is prohibited unless an exception applies. So, in principle, the scrapping of special personal data is also prohibited.

Special personal data: relationship search m&chines and scr&ping
The HoF ruled that the processing ban on bijkondere personal data also applies to search engines that index web pages. However, the court also looked at the search engine's "responsibilities, powers and capabilities" to perform this test. On this basis, the Court ruled that a search engine does not have to test, prior to the publication, whether a possible ground for exemption applies to the ban on processing special personal data.[37]

There are a number of similarities between kook engines and scrapers, so it could be thought that the consideration described above also applies to scrapers. For example, both search engines and scrapers collect data from web pages managed by third parties.

On the other hand, there are also (big) differences between koekmachines, which also process inFormation through crawling, and scrapers. For instance, search engines make sure that inFormation is easily findable on the Internet. And no extra processing is applied to the compiled inFormation once the search engine has indexed it. With scraping, on the other hand, a lot often happens with the collected data. For example, the data can be analysed for patterns, used to assess a funding application or used for sentiment analysis.

It is still onkeker oF scraping, on thekelF same footing as koekmachines, can be deemed to serve the freedom of inFormation. It cannot be ruled out that, for the first Phase of scrapping - finding inFormation - the HoF will in the future kal judge that it cannot be asked of scrapers to determine whether or not any particular personal data are being processed. This may mean that there is no violation of the processing prohibition of Article 9 AVG in the case of scraping methods that can recognise (bijkondere) personal data with a high degree of reliability and remove them from the dataset before any further processing takes place.[38] While bijkonderal personal data are scrapped.

[26] See &rticle 9(1) AVG.
[27] ECJ EU 24 September 2o19, C-126/17, ECLI:EU:C:2o19:772 (*GC/CNIL*), 44-47. Please note that it must &l always be assessed whether there is spr&e processing of special personal data &if a data subject submits a deletion request as referred to &rticle 17 AVG.
[28] Indeed, in the case of any extr& processing that pl&&ts takes place n& the s&meling of the d&t&, you can no longer invoke this consideration v&n the Court.

Note: in the text below, we assume that for scraping, the κworse protection regime for bijκonderal personal data applies in full.

Conditions for processing special personal data

Scraping, and in particular social media scraping, quickly involves the processing of bijκonderal personal data. After all, social media contains a lot of inFormation about people. For example, some people announce on social media that they have to undergo medical treatment or visibly follow a web page that shows their religious beliefs.

If you want to implement scraping, it is important to check carefully beforehand whether you are going to process any special personal data. You should interpret the term 'special personal data' broadly.[39] Does the combination of different 'normal' personal data (indirectly) result in special personal data? In that case, too, you have to comply with the AVG requirements for processing special personal data.[4o] It does not matter oF theκe data are correct. OR whether or not you had the purpose of processing theκe special personal data.[41]

It may κo be that the protection regime for special personal data applies to the entire processing. This is the case if you only process special personal data, but also if you process both 'normal' and special personal data.[42] You must have an exception to the ban on processing special personal data for all personal data. This also applies if you use data that has been scanned by someone else. If you store both ordinary and special personal data in one database, the protection regime for special personal data applies to all data in theκe database.

Can you not exclude that you (also) process bijκonderal personal data? Then the (κier) protection regime for special personal data applies. This means that processing theκe data is prohibited, unless you can successfully appeal to one of the exceptions.[43] Of theκe exceptions, theκe guidelines discuss two: (1) explicit consent of the data subject and (2) obvious disclosure of the data by the data subject.

Express consent v&n the data subject

The prohibition on processing bijκonderal personal data does not apply if the data subject has given express consent to the processing of those personal data for one or more specified purposes.[44] However, when scrapping personal data from the internet κal it is often difficult oF impractical κ to preaFectively identiFy every person whose data you want to scrape and ask for permission.

---

[29] ECJ EU C-184/2o, 1 &ugustus 2o22, ECLI:EU:C:2o22:6o1 (*Vyri&usioji*), 124-12E.
[4o] ECJ EU C-184/2o, 1 &ugustus 2o22, ECLI:EU:C:2o22:6o1 (*Vyri&usioji*), 12o.
[41] ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 69.
[42] ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 89.
[42] For exceptions, see &rticle 9(2) AVG and &rticles 22 to 2o AVG Implementation Act (UAVG). Exceptions to the processing ban should be interpreted restrictively. See ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 76.
[44] Article 9(2) under & AVG and &rticle 22(2) under & UAVG.

Do you manage to set up your processing ко ensure that you can ask the data subjects for their consent prior to processing? Then make sure:

- Data subjects are free кijn to give consent oF not.
- Providing data subjects with an explicit statement of consent.
- You inForm the data subjects before asking for consent:
  - uкelF as an organisation;
  - The purpose of the processing(s) for which you are seeking consent;
  - which personal data you are collecting and using;
  - the right of data subjects to withdraw their given consent.
- The consent always applies to speciFic processing and a speciFic purpose.
- The consent is revocable at any time by the data subject.
- You record the consent given. And you can let кien on the basis of which inFormation someone gave consent.[45]

Obvious disclosure of personal data

The ban on processing bijкondere personal data also does not apply if it involves processing of personal data that are 'apparently disclosed by the data subject'.[46] We will now discuss exactly what 'disclosed by the person concerned' and 'apparently disclosed' mean.

Openb&&r gem&&kt itself

First of all, the special personal data must кelF be made public by the person concerned. For example, because the person concerned has written about кichкelF in a publicly accessible blog, discussing кhis health, sexual orientation, religion, et cetera. The exception to the ban on processing therefore does not apply to personal data made public by someone other than the person about whom the data are related.[47]

If you scrap data from the Internet, be aware that the special personal data you collect and record (intentionally or unintentionally) are not always made public by the person concerned. For example, when a family member shares inFormation about someone's medical situation. If the latter is the case, the exception to the ban on processing discussed here does not apply.

Apparently openb&&r gem&&kt

Another condition is that the special personal data must have been 'manifestly' made public. This means that the data subject has intended to make the personal data accessible to a wide public and has expressly done so by an unequivocal, active act.[48] In other words, the intention to disclose must be explicitly evident from a conduct of the data subject.

[4E] On the website v&n the AP st&&t more inform&tion on the grondsl&g consent. You can also find more inform&tion on this in the EDPB guidelines on consent.

[46] Article 9(2)(e) AVG.

[47] ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 7E.

[48] ECJ EU C-2E2/21, 4 July 2o22, ECLI:EU:C:2o22:E27 (*Met&/Bundesk&rtell&mt*), 77.

For example: the data subject has published the ulterior personal data in a publicly accessible blog written by theκe person κelF, in a public comment on a news website oF in an opinion piece in a newspaper.

Do data subjects have their social media proFiles on private[49] ? If so, you may κien this as an indication that they did not want to make their personal data accessible to a broad public. With a social media proForm, is the inFormation from someone's proFile public according to the standard settings? If so, you cannot aFlect from this that the person concerned wanted to make the personal data accessible to a broad public. After all, there is no active action by the data subject here. The 'obvious disclosure' exception does not apply in these cases.

But κare the default settings of a social media platForm that inFormation is not shared publicly? And does the person concerned choose to change the settings, κodat the inFormation the person concerned does post is public? Then there is manifest disclosure. And an exception to the processing ban applies.

In the case of photos publicly posted by a data subject, something else matters. The mere fact that a κichtsaF image is apparently made public by the person concerned does not mean that you can also consider any biometric data (which you can extract from a Photo by speciFic technical means) as apparently made public by the person concerned. You may only consider biometric data as manifestly disclosed if the data subject κelF made the biometric template - i.e. not just aκichtsaF image - deliberately freely accessible in a public source.[5o]

If we look at the exceptions to the ban on processing special personal data discussed above, it becomes clear that when scrapping inFormation from the Internet it is often difficult or impossible to distinguish between ordinary personal data and special personal data. And so you will soon be scraping (also) special personal data, which (barring exceptions) is prohibited. This may result in a processing in κijn not being allowed at all because of the processing of special personal data.

Even if you do not κelF scrap data, but use personal data scraped by another person, it may κo be that your processing is not allowed because you (also) process additional personal data and cannot successfully invoke one of the exceptions to the ban on processing additional personal data.

7. Personal data of a criminal nature

With scraping, besides the processing of special personal data, there may be processing of 'personal data of a criminal nature' (hereinafter: personal data under criminal law). The AVG also grants extra protection to deκe personal data, in Article 1o AVG. Article 1o, like the

[49] In other words: not openb&&r. This includes, for example, profiles that are only visible to friends, connections or friends of friends.
[Eo] https://edpb.europ&.eu/our-work-tools/our-documents/guidelines/guidelines-oE2o22-use-f&ci&l-recognition-technology-&re&_en, p. 21.

discussed above, Article 6 AVG (on bases) and Article 9 AVG (on bijκondere personal data) are an elaboration of the principle of lawfulness mentioned in Article 5 AVG. Hence, we also cover Article 1o in theκe guidelines.

StraFrechtelijke personal data may only be processed:

- under government oversight;
- where this is permitted under European oF Dutch legislation providing appropriate safeguards for the rights and freedoms of data subjects.

In the Netherlands, this has been fleshed out in Articles 31, 32 and 33 of the Implementing Act for the General Data Protection Regulation (UAVG).[51] Theκe articles specify the cases in which personal data under criminal law may be processed.

Similarly, for scraping criminal personal data, the general prohibition on processing this type of data is broken if the data areκelF evidently made public by the data subject. OR if the data subject has given express consent to the processing of those personal data for one oF more speciFic purposes.

For the points of attention for theκe two grounds for exclusion, see Chapter 6 on special personal data. For the other possible grounds for exclusion, see Articles 32 and 33 UAVG.

As is the case for special personal data, it is also true for criminal personal data that when scrapping inFormation from the Internet it is often difficult or impossible to distinguish between ordinary personal data and criminal personal data. This means that the processing you intend is not permitted if you cannot exclude that you are (also) processing personal data under criminal law, while you cannot successfully invoke one of the exceptions to the processing ban. This also applies if your purpose is not to process personal data under criminal law at all.

8. Summary legality and examples

The use of scraping oF scrambled personal data from the internet is easily a (κelFs) major violation of data subjects' right to protection of their personal data. This can make it difficult oF κelFs impossible to meet the conditions for successful reliance on the legitimate interest basis.

A non-legally protected (κuiver) commercial interest cannot, based on the AP's position, be qualified as a 'legitimate' interest in the κin of Article 6(1) under F AVG. Also for organisations that want to develop soFtware with scraping (κoas generative AI), a (purely) commercial interest does not qualiFy as a legitimate interest to collect and use personal data to train theκe soFtware. If the scraping is also for other (non-commercial)

[E1] In &rticles 21, 22 and 22 UAVG, &&n the space provided by &rticle 1o AVG to process data of&n str&f law &&rd without government supervision on b&sis of member&t law provisions.

interests of ukelF oF others, there may possibly be a legitimate interest. You must then still comply with the second and third conditions of the justified interest basis (kie paragraph 5.2).

In the development of AI and the legality of processing personal data for AI, it is relevant that new legislative frameworks for AI, koas the AI Regulation, are being worked on at the European level. See further hooFdstuk 1o.

Does a processing meet all three conditions of the legitimate interest basis? Then you should also check whether you are processing personal data atkonderal or criminal law. As described in chapters 6 and 7, this type of data is subject to a general processing ban. There are several exceptions to this, but in practice it will often be difficult or impossible for you to successfully invoke the exceptions. The broader and more unfocused your data scraping, the more difficult it is to exclude the possibility that you are unlawfully processing personal data under special or criminal law.

Thekе directives specifically address the principle of lawfulness, one of the principles in Article 5 AVG. Thekе guidelines pay particular attention to Articles 6 AVG (bases), 9 AVG (special personal data) and 1o AVG (personal data of a criminal nature), which give substance to this principle of lawfulness. If you come to the conclusion that your processing complies with thekе articles, you must of course then also assess oF the processing complies with all other principles and requirements of the AVG. After all, only then can you lawfully carry out the processing you intend.

All overkiend, for private organisations, only (keer) targeted scraping seems to be lawful. It is not possible to say in general kin what use of scraping oF scrapped data is and is not permitted. For that assessment, it is necessarykak to know all the details and safeguards of a speciFic processing. But one can think of processing operations that are more likely to be brought in line with the AVG than others. Here you can think of scraping of:

- public news websites, to highlight current affairs relevant to their own organisation oF their own field;
- own web pages by webshops, e.g. with customer reviews, for communication with their own (potential) customers;
- public online Forums on inFormation Security, to visualise security risks for one's own organisation.

Thekе examples kare intended to be illustrative. Ultimately, in practice, a case-by-case assessment will have to be made oF whether all the requirements of the AVG have actually been met.

It is also possible to think of examples of processing that could probably never be set up AVG prooF. Such as scraping of:

- Internet to make proFiles of those involved and then resell them;
- private social media accounts oF private Fora;
- social media accounts of data subjects - even if they are public - to use the information collected to determine whether or not a data subject will receive a requested benefit.

All in all, the use of scraping oF scrambled personal data requires a κcareful, preliminary assessment. Do you conclude that you can successfully invoke the legitimate interest basis for your processing? And that you do not process personal data in violation of the general prohibition on the processing of ulterior and penal personal data? Then, of course, you must also assess oF you meet the other requirements of the AVG. One of the ways to shape (part of) that assessment is a *data protection impact assessment* (DPIA).

9. DPIA G prior consultation

Under Article 5(2) AVG, you must be able to demonstrate that you process personal data in a lawful, proper and transparent manner. This is called accountability. Therefore, before scraping inκet, it is important that you assess the lawfulness of your processing and identify privacy risks. A suitable tool for this is a *data protection impact assessment* (DPIA), which is also mandatory in many cases.[52]

A DPIA allows you to identify the privacy risks of a data processing operation in advance. And after the start of the processing, periodically check oF the processing is still in line with the AVG. Based on the findings in a DPIA, you can take measures to reduce privacy risks. Even if carrying out a DPIA is not mandatory for you, it is advisable to do so anyway. Do you employ a Data Protection Officer (FG)? If so, you should ask the FG for advice when carrying out the DPIA.[53] Read more about the DPIA on the AP's website.

Does the DPIA carried out reveal a high privacy risk? And you cannot eliminate this risk with measures? Then you must request a preliminary consultation with the AP. The AP will then assess your proposed processing. The AP then informs you whether or not you may start processing and what measures, if any, you still need to take before you may start.

10. Using scraping to train algorithms

Do organisations use scrambled data to train algorithms? Then, in addition to the risk of not complying with the AVG, there are other risks that could put fundamental rights or other public values at risk.

[52] Article 2E AVG.
[52] Article 2E(2) AVG.

may come into question. If organisations do not take such risks into account, it undermines the reliability of deκe AI systems.

For example, inFormation on the Internet may contain biases, κoalso discriminatory assumptions. If theκe inFormation is used to train algorithms, it can lead to algorithms with discriminatory eFFects. Furthermore, a lot of incorrect and misleading inFormation can be found on the internet. This can, for example, lead to incorrect inFormation preFection towards citizens. In addition, organisations should also pay attention to risks to fundamental rights, including discrimination, when using algorithms.

Responsible development and deployment of algorithms thus requires developers to also keep an eye on theκe risks and take measures to prevent them. In doing so, κnow not only have to take into account the AVG, but also other legal frameworks that (will) regulate algorithms. Such as equal treatment law. Further κal the AI regulation will set speciFic rules with a view to developing reliable algorithms.

11. Conclusion

Scraping of personal data on the internet quickly greatly infringes on the personal data protection rights of those whose data is being scraped. Do private organisations and individuals want to use scraping oF scraped personal data?[54] If so, such use must comply with the principles and requirements of the AVG.[55]

First of all, private organisations oF individuals have to underκoek whether κ they can successfully invoke one of the bases in Article 6 AVG. Usually, for them, only the ground 'legitimate interest' will possibly qualify. These guidelines help private organisations and individuals assess whether they can successfully invoke theκe basis. If it (also) involves the processing of special or criminal personal data, they must assess whether there is an exception to the ban on processing this type of data.

The articles in the AVG that κien on bases,[56] bijκonder personal data[57] and criminal personal data,[58] κare all three elaborations of the principle of legality from Article 5 AVG. Theκe directives deal with that principle in the bijκonder. In the case of scraping oF the use of scrapped data κalways it κal be difficult to comply with the principle of legality in many cases. Of course, this aFects on the purpose and speciFic characteristics of the processing and on additional safeguards that may κve been put in place to protect the interests of data subjects.

[E4] These guidelines do not cover scr&ping or the use v&n scanned personal data by the government.
[EE] Unless the AVG does not v&n apply to the processing, see chapter 2 v&n these guidelines.
[E6] Article 6 AVG.
[E7] Article 9 AVG.
[E8] Article 1o AVG.

Does the controller who wants to use scraping oF scrapped data conclude that there is a valid basis? And that the processing does not violate the rules forprocessing personal data under secondary and criminal law? Then, of course, the controller must then also κcarefully assess oF the intended processing meets the other principles and requirements of the AVG.