noyb - European Centre for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

IMY
Integritetsskyddsmyndigheten
Box 8114
104 20 Stockholm
+4686576100
imy@imy.se

[redacted]

noyb Case-No:	C-077
Complainant:	[redacted]
Represented under Article 80(1) GDPR by:	*noyb* - European Centre for Digital Rights Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria
Respondent:	Nusvar AB (www.mrkoll.se) Luntmakargatan 66 113 51, Stockholm, Sweden
Regarding:	A violation of, among others, Article 6, 14 and 17 GDPR. As well as a question about the compatibility of Swedish and EU Law.

COMPLAINT UNDER ARTICLE 77 GDPR

1. REPRESENTATION

1. *noyb* - European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *"noyb"*) **(Attachment 1).**

2. *noyb* is representing the data subject under Article 80(1) GDPR (hereinafter, also *"the complainant"*) **(Attachment 2).**

2. FACTS OF THE CASE

2.1 Foreword

3. The Swedish implementation of Article 85 GDPR is **problematic**. To protect freedom of expression, Swedish national law exempts the media sector from the scope of the GDPR. To benefit from this protection a company simply has to apply for a media licence, which is granted without any screening related to the purpose of the processing. Consequently, data brokers whose business models have nothing to do with freedom of information and expression (like the controller in this case, hereinafter also "*MrKoll"*), receive such licenses and operate outside the scope of the GDPR. This is a clear violation of EU law for the reasons set out below.

2.2 The controller - MrKoll

4. On its website www.mrkoll.se (hereinafter also, the *"Website"*), the controller describes its activity with the following words: *"Mrkoll is a search service for information on private individuals, developed for consumers. We collect information from public registers and process it to make it easy to understand. We compile information on people aged 16 or older. In total, around **8.4 million individuals** are searchable in the service."* (emphasis added)[1] (**Attachment 3**)

5. In other words, MrKoll obtains information on the entire Swedish population from public authorities, organises and arranges it in an easily searchable fashion, and sells it to **anyone** interested.[2] The information includes, among the others, first names, surnames, residential addresses, real estate values, **telephone numbers**, **cars owned**, company registration numbers, **criminal records**, civil proceedings and **minor offences** committed by Swedish residents.

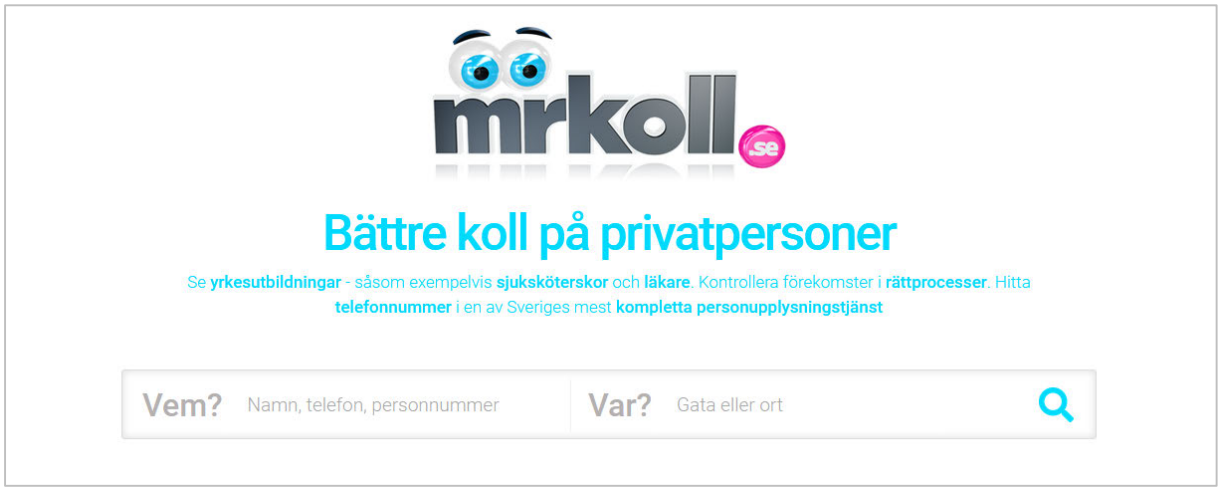
6. The website's home page bears MrKoll's logo, surmounted by two eyes in stylised form. The scrutinising eyes refer to the idea of the search for information. The word *"Koll"* comes from the Swedish verb *"Kolla"* which means "to check". This is confirmed by the service's slogan, *"Better control of private individuals"*[3] and by the examples provided on the information page, *"Keep track*

[1] Translation from the original Swedish: "*Mrkoll är en söktjänst för information om privatpersoner, utvecklad för konsumenter. Vi samlar information från offentliga register och hanterar den för att göra den lättförståelig. Vi sammanställer information om personer som är 16 år eller äldre. Totalt finns cirka 8.4 miljoner individer sökbara i tjänsten*."

[2] There is no need to show a specific interest in knowing the information sold on the website. The "customer" simply looks up an individual and buys whatever information they are interested in.

[3] Translation from the original Swedish: "*Bättre koll på privatpersoner*."

of who is moving in!",[4] *"Who is the most searched person?"*.[5] The introduction to the website also states *"See vocational training - for example nurses and doctors. Check occurrences in legal proceedings, find phone numbers in one of Sweden's most comprehensive personal information services."*[6] (see, Attachment 3).



7. In the section "*Certificate of use*"[7] MrKoll specifies that it has obtained a publication license from the Swedish press authority. According to the controller, this means that their *"publications and so-called database (the entire Mrkoll.se website) are covered and protected by the* [Swedish] *Fundamental Law on Freedom of Expression (YGL)"* and that *"**the GDPR does not apply to the Mrkoll.se service** or other services that have been granted a publishing licence - which possess the same constitutional protections as mass media.*[8] (emphasis added) (**Attachment 4**).

8. Thus, according to the controller, selling personal information about Swedish citizens and residents is *tantamount* to expressing ideas, thoughts, or feelings, or even practising journalism. Below, *noyb* refutes this assertion.

---

[4] Translation from the original Swedish: "*Håll koll på vem som flyttar in!*"
[5] Translation from the original Swedish: "*Vem är mest eftersökt?*""'*Eftersökt*" refers to someone who is searched for and can be used as a synonym to "*efterlyst*" which in turn means "wanted" (as in wanted by the police). So, the Swedish phrasing recalls criminal investigations, probably as part of the morbid appeal of the site.
[6] Translation from the original Swedish: *"Se yrkesutbildningar - såsom exempelvis sjuksköterskor och läkare. Kontrollera förekomster i rättprocesser. Hitta telefonnummer i en av Sveriges mest kompletta personupplysningstjänst."*
[7] Translation from the original Swedish: *"Utgivningsbevis".*
[8] Translation from the original Swedish: "[P]*ublicering och den s.k. databasen (hela webbplatsen Mrkoll.se) omfattas och skyddas av grundlagen om yttrandefrihet (YGL)*" and that "*att GDPR inte gäller för tjänsten Mrkoll.se eller andra tjänster som har tilldelats utgivningsbevis - som därmed besitter samma grundlagsskyddade massmedier.*"

2.3 Relevant Processing Operation

9. On 4.10.2023, the complainant (hereinafter also referred to as "*data subject*") visited the MrKoll website to check how it worked. As announced on the Site (§§ 4, 5 and 6 above), MrKoll provides personal information based on different levels of "depth". The first level, accessible to anyone visiting the website, presents general information on the individual profile.

10. For example, by simply searching someone by name, the data subject discovered that [redacted] is born on [redacted] and is a doctor by profession. MrKoll provides [redacted] phone numbers [redacted] and [redacted]) and address ([redacted]. **MrKoll also provides insights into anyone's co-habitant.** For instance, [redacted] lives with her partner [redacted] (**Attachment 5**). [redacted], in turn, age 68, is the owner of two cars, registered in 2016 and 2021, both grey, as well as of the home he shares with [redacted] The marital home has a surface area of [redacted] square metres and a market value of between EUR [redacted] million (**Attachment 6**).

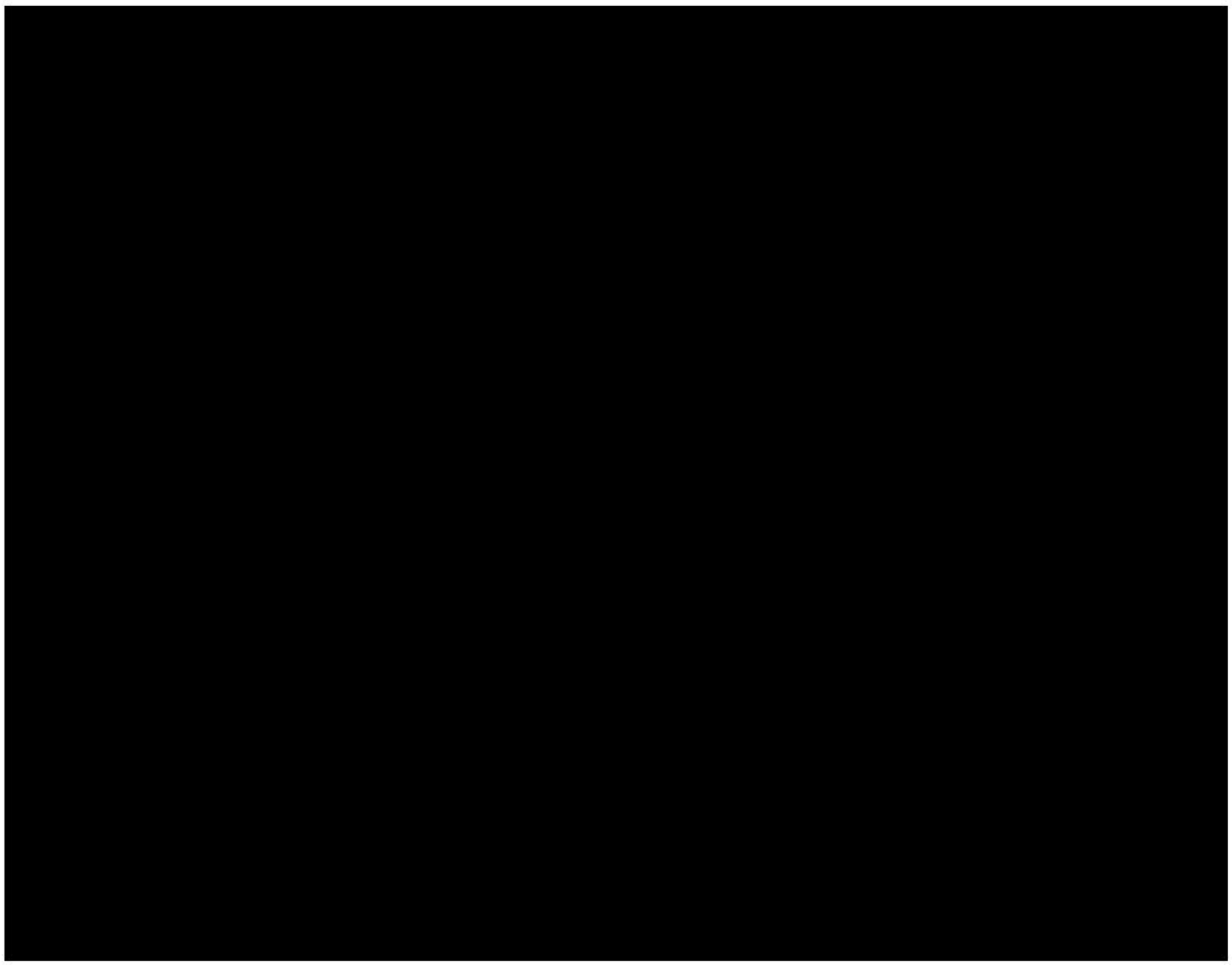
11. The information available on MrKoll, however, is not limited to addresses, phone numbers, real estate and cars. By paying a further sum of money, the visitor can access a second level of detail and obtain information about criminal records, civil judgments and penalty orders against almost any Swedish resident.[9] Paying again grants access to a final layer of information, since those judgements (if any exist) become fully accessible to the payee.

12. For example, the data subject searched for the profile and paid for the criminal records of his acquaintance (*Ms A*) who, according to the controller, had been implicated in 7 criminal cases and one civil judgment (**Attachment 7**). Upon paying, the controller gave the complainant a more detailed report of Ms A's entire criminal history, mostly involving her complicated relationship with a former partner.[10] The report provided by MrKoll informs about the continuous quarrels between the partners, the use of strong and aggressive terminology, alleged threats, extortion, damage as well as the abuse of alcohol and other substances. Among this information is Ms A's alleged blackmail over the custody of her young daughter Y, whose **full name and date of birth** is provided on several occasions in the court records (**Attachment 8**).

[9] According to an article found online, in the preceding months, 36 Swedish district courts have handed over a total of 223,250 criminal convictions handed down between 2017 and 2022 to the company Bakgrundskollen.se, a data broker providing a similar service to MrKoll. See, https://www.svt.se/kultur/hd-mal-med-mrkoll-ska-provas-igen (last accessed on 22.1.2024).

[10] The purchaser can read a total of 8 cases involving Ms A. For each case the purchaser is given the option to download the full judgement.

13. MrKoll also presents a page of **the most searched profiles** on the platform (**Attachment 9**). Not only are the names of actors or politicians found there, but also those of ordinary citizens.



14. To cite one case, on 4.10.2023, the most sought-after profile was that of Mr [redacted], aged [redacted], resident in [redacted] at [redacted]. Upon paying, the complainant discovered that Billy was involved in 7 criminal proceedings as a suspect (**Attachment 10**). Mr [redacted] profile was particularly in demand as news had broken of [redacted] involvement in serious crime. The 22-year-old, in affiliation with the neo-Nazi movement, had been charged for the killing of three people with an explosive device for reasons of racial and political hatred (**Attachment 11**). However, since MrKoll provides details about co-habitants (§ 10 above), the second and third profiles on the list corresponded to [redacted] and [redacted]. Most likely members of the same household and residing at the same address. These elements were enough to arouse the public's curiosity and to place these two women, in all probability unrelated to the deeds committed by [redacted], in the "spotlight".

15. Position no. 12 on the list of 4.10.2023 featured Mr [redacted]. The numerous hits were probably due to the involvement of [redacted], owner of a car dealership, in a fraudulent bankruptcy affair in which members of his own family were also involved (**Attachment 12**). A news article about the facts was published on *Flashback.org* and commented on by the user [redacted] with the sentence "*Family business is nice!*" The same user "enriched" the news by revealing that, according to his search on MrKoll, one of the members of said family (whose implication in the bank-

ruptcy was far from proven) still lived in the family residence. In response, another user commented "*There will be many addresses that the military will have to protect.... Time to increase Swedish defence!!! Military on our streets now!*"[11] (**Attachment 13**).

16. Unwilling to contribute to MrKoll's questionable mission, on 5.10.2023, the complainant requested the removal of all his personal data (**Attachment 14**) from MrKoll's website under Article 17 GDPR: *"Hi I would like you to remove me from the database*"[12] (**Attachment 15**). A few hours later, MrKoll rejected the request. As already announced on its website (§ 6 above), the controller stated, *"the database is **not affected** by the General Data Protection Regulation (GDPR)."* (emphasis added). In particular, "*there is currently **no possibility to permanently remove any data from MrKoll**, unless you have a protected identity or a confidentiality mark in the population register.*"[13] (emphasis added) (**Attachment 16**).

17. The facts and the examples above highlight a serious violation of the complainant's (and **millions** of Swedish residents and citizens') right to protection of personal data. The controller uses the constitutional protection afforded to freedom of expression and journalism to grant itself a blanket exemption from the GDPR.

18. The problem is that MrKoll is, to all intents and purposes, a **data broker** and its activity **does not deserve such constitutional safeguards.**

3. GROUNDS FOR THE COMPLAINT

3.1 The Swedish Implementation of Article 85 GDPR

19. To understand why MrKoll can wrongly invoke such constitutional safeguards, and why such safeguards are neither appropriate nor in line with EU law, it is necessary to conduct a brief analysis of the Swedish regulation of online publications.

20. Article 7 of Law 2018:218 implementing the GDPR into the Swedish legal system (hereinafter, also "*DSL*") stipulates as follows:

> *1. The EU's data protection regulation and this law shall not be applied to the extent that it would **conflict** with the freedom of the press regulation or the freedom of expression fundamental law.* (emphasis added)

21. Thus, according to the Swedish implementation law, the GDPR does not apply in the case of "*conflict*" with the Basic Law on Freedom of Expression (hereinafter, "*YGL*"). The purpose of the YGL is to ensure the free exchange of opinions and information, as well as maximum freedom of

[11] Translated from the original Swedish: "*Det blir många adresser som militären måste skydda... Dags att öka svenska försvaret!!! Militärer på våra gator nu*!"
[12] Translated from the original Swedish: *"Hej jag skulle vilja att ni tar bort mig från databasen."*
[13] Translated from the original Swedish: *"innehar ett så kallat frivilligt utgivningsbevis påverkas databasen inte av Dataskyddsförordningen (GDPR)."* In particular, *"Detfinns i dagsläget ingen möjlighet att permanent ta bort några uppgifter från Mrkoll, såvida man inte har skyddad identitet eller en sekretessmarkering i folkbokföringen."*

artistic expression (Article 1:1 YGL). Consequently, whenever the GDPR limits this purpose, one can, at least in theory, imagine a "*conflict*" with the YGL.[14]

22. According to Section 1:4(1) YGL, the protection also extends to, among others, the transmission and publication of information contained in a "*database*" by:

> *(a) the editorial office of a printed periodical or a programme;*
> *(b) an enterprise for the professional production of such printed matter referred to in the Freedom of the Press Act or of technical recordings;*
> *(c) a news agency;* ***or***
> ***(d) someone else, provided there is a certificate of no legal impediment to publication for the activity under Article 5;*** (emphasis added)

23. In cases (a), (b) and (c) above, the intent is clearly to extend constitutional protection to online archives typical of "classic" journalism.[15] However, Article 1:4(1)(d) YGL, highlighted above, also extends the protection to **anyone** in possession of a so-called "*certificate of no legal impediment*".[16] The requirements for obtaining such a certificate are laid down in Article 1:5 YGL. These requirements are rather "flexible":

> *A certificate of no legal impediment to publication is issued if:*
> *1. the activity is organised in the manner referred to in Article 4 and transmissions emanate from Sweden;*
> *2. a qualified responsible editor has been appointed and has accepted the appointment; and*
> *3. the activity has a name such that it cannot easily be confused with the name of another activity under Article 4.*

In practice, almost anyone can obtain this certificate and, by doing so, benefit from the constitutional protection guaranteed by Article 1:4(1) YGL.

24. It is because of such legislative dynamic that controllers like MrKoll can publish and sell personal data while enjoying the constitutional protection guaranteed to the media. In other words, the mere possession of the "*certificate of no impediment*" equates MrKoll, a data broker, with newspapers, TV news, cultural magazines, and investigative articles.

25. The above protection, however, is not absolute. YGL, contains exceptions to the right of free expression of ideas and balances it against other legal interests of constitutional relevance:

> "[The YGL] *also describes what is not permitted, for example defaming or publicly insulting another person. The Law has been extended to keep pace with the development of new media. If something is conveyed that may be regarded as agitation against a population group or if a film is shown which contains elements of sexual violence, these may be possible offences against the Fundamental Law on Freedom*

---

[14] According to MrKoll, a controller with a media license obtains, pursuant to Article 7 DSL, a blanket exemption from the GDPR. It does not matter whether the published information is in the public interest, or whether there is an appropriate legal basis. In MrKoll's reading, the mere fact of possessing a license exempts the controller from any obligation under the GDPR.

[15] "*The Fundamental Law on Freedom of Expression applies to radio, television, films, sound and picture recordings, video and CD recordings, as well as websites and blogs* ***with a journalistic focus.***" (emphasis added) (https://www.riksdagen.se/en/how-the-riksdag-works/democracy/the-constitution/#the-fundamental-law-on-freedom-of-expression-3) (last accessed 1.2.2024)

[16] This is the so-called "*Utgivningsbevis*" referred to in § 7 above.

of Expression. The same applies to possible threats to the security of the country or society through the publication of something involving, for example, espionage."[17]

26. Technically speaking, under Article 1:1(2) YGL, limitations to freedom of expression are possible provided there is a provision to that effect within the YGL itself. Regarding the relationship between freedom of expression and data protection specifically, this provision is Article 1:20 YGL:

> 1. *Notwithstanding the provisions of this Fundamental Law, rules may be laid down in law concerning bans on the publication of personal data:*
> *1. which reveal* ***ethnic origin, skin colour*** *or other similar circumstance, political opinions, religious or philosophical conviction or membership of a trade union;*
> *2. concerning* ***health, sex life or sexual orientation****;*
> *3. which consist of* ***genetic data or biometric data*** *enabling the unambiguous identification of a natural person.*
>
> 2. *The provisions of paragraph one only apply if:*
> *1. the personal data are included in a data collection that has been arranged in such a way that it is* ***possible to search for*** *or compile the data; and*
> *2. with regard to the nature of the activities and the forms under which the data collection is made available, there is a* ***particular risk*** *of improper violation of individuals' personal privacy.*

27. The provision in question outlines the constitutional boundaries between freedom of expression and processing of personal data. Under Article 1:20 YGL, limitations are allowed only when processing concerns special categories of data (including, ethnicity, skin colour, political opinions).[18] Under Article 1:20 YGL, if this requirement exists,[19] freedom of expression **can** be restricted and consequently **no** "*conflict*" between the GDPR and YGL is held to exist. By comparison, when the above requirement does not exist, freedom of expression "re-extends" its domain, so to say, and the GDPR (according to Article 7(1) DSL) no longer applies because it is considered to be in "*conflict*" with the YGL.

3.2 The Swedish Framework is incompatible with EU law for (at least) two reasons

28. This, in brief, is the Swedish system. It should be emphasised at the outset that this solution appears to be at odds with European law for at least two reasons:

1. The mechanism of "*certificates of no impediment*" inherently allows non-journalistic entities to obtain a blanket exemption from the GDPR in violation of EU law.

2. Swedish law unreasonably permits privacy to be balanced against freedom of expression only when sensitive data is involved.

---

[17] See, https://www.riksdagen.se/en/how-the-riksdag-works/democracy/the-constitution/#the-fundamental-law-on-freedom-of-expression-3 (last accessed, 2.1.2024)
[18] The list under the YGL is comparable with the types of data covered under Article 9 GDPR. Hence, the reference to "*special categories of data*".
[19] Alongside the other two requirements outlined in Article 1:20(2) YGL.

3.2.1 The problem of certificates of no impediment in relation to the GDPR

29. In short, from the preceding paragraphs. Pursuant to Article 1:5 YGL, MrKoll receives a "*certificate of use*" or "*no impediment*". The controller does not engage in any journalistic activity. However, the mere fact of owning the certificate gives MrKoll access to constitutional protections reserved for traditional media. Among these protections, under Article 7 DSL (§§ 19-23), there is an almost total exemption from the GDPR.

30. This situation is in open conflict with EU law.

31. Under Article 85(1) GDPR, a Member State is required by law to **reconcile** the right to protection of personal data with the right to freedom of expression and information by making specific derogations to the GDPR. Under Article 85(2) GDPR, to be permissible, derogations must be **necessary** to strike a proper balance between freedom of expression for **journalistic, artistic, and academic purposes**[20] and the protection of personal data (i.e., the GDPR).[21] The relationship between two paragraphs of the provision is as follows: Article 85(2) GDPR determines how the reconciliation referred to in paragraph 1 is to be accomplished. In other words, exceptions to the GDPR are only possible when the expressive form has a journalistic, artistic, or academic purpose, broadly understood, according to the instructions of the CJEU and ECtHR.[22]

32. In this context, the definition of "*journalism*" is, **crucial.**[23] If a processing operation is **not** carried out for journalistic purposes, then the exemption cannot be "*necessary*" by definition. Hence, a Member State will not be able to adopt an exemption which **does not** relate to journalistic purposes without violating the GDPR.

33. Regarding the definition of journalism, the most relevant instructions come from the European Court of Human Rights.[24] According to Strasbourg case law, particular attention must be paid to the **purpose** of a certain expression. In general terms, where the information is intended to stimulate a debate on a topic of **general interest**, it is possible to see a journalistic purpose. Conversely, there is no journalism when the purpose is to merely "***satisfy the curiosity of a particular readership*** *regarding the details of the applicant's private life,* [since this] *cannot be*

---

[20] Under Article 85(2) GDPR, exemption from the GDPR is **only** possible when the processing is carried out for "*journalistic purposes* [...]". Article 85(2) GDPR. This also applies to academic and scientific purposes.

[21] This dynamic is quite normal. Data protection can, if used in abusive terms, be a tool to unacceptably restrict the free debate of ideas within a democratic community. The classic example is that of a data subject, e.g. a politician, requesting under Article 17 GDPR to have his or her name deleted from an online newspaper article in which he or she is subject of a report on corruption concerning him or her. Such a request would be abusive as it would unduly restrict the journalist's freedom of expression to inform (and the public to be informed) about a relevant news story. For these reasons, Article 85(2) GDPR allows (requires) the Member State to adopt any derogation necessary to protect freedom of expression for journalistic purposes.

[22] The academic commentary agrees that Article 85(1) GDPR should not be read as requiring member states to reconcile data protection with freedom of expression and information in areas which are **not** linked to the purposes outlined in Article 85(2) GDPR (journalism, academia, art). See, among the others, *Spiecker et al.*, GDPR Article-by-Article Commentary (2023), p 1074. For example, a proposal by the European Parliament to impose a duty on Member States to balance data protection and freedom of expression and information independent of any specific purposes of processing was not adopted.

[23] Since MrKoll is neither (and does not claim to be) an academic paper, work of art or literature, it can only rely on journalism as the basis for its alleged "exemption". The legal definition of journalism and consequently journalistic purpose will be presented below.

[24] Under Article 52(3) of the EU Charter of Fundamental Rights**,** "*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*" The interpretation given by the European Court of Human Rights is therefore relevant to the present case.

deemed to contribute to any debate of general interest to society despite the applicant being known to the public. (ECtHR, 24.09.2004, *Von Hannover v Germany*, 59320/00, § 65).[25]

34. In addition to the above requirements, the ECtHR has developed further criteria that can be used when balancing privacy and freedom of expression. These include the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity (ECtHR, 27.06.2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 931/13, § 165). Similarly, another element is "*the possibility for the controller to adopt measures to mitigate the extent of the interference with the right to privacy must be taken into account.*" (CJEU, 14.2.2019, *Buividis*, C-345/17, § 66).

35. That clarified, the information on MrKoll and, more generally, its business model, plainly **fall outside** the definition of "journalism". The personal phone number of a Swedish woman does not inform the public debate. The number of cars owned by her husband, or the value of their home, only feeds public curiosity. The judicial account of a twisted relationship between a woman and her toxic ex-partner is of no public relevance. Even worse, if this account includes her young daughter whose full name and date of birth are fully available to anyone who has paid for her mother's court records. Further, publishing the name of two women whose only 'fault' is sharing an address with a racist, violent individual, is not journalism. The same applies to the family members of an individual accused of fraudulent bankruptcy. MrKoll has no "*measures to mitigate the extent of the interference*" for these people.[26] Rather, the controller denies their fundamental rights guaranteed by the GDPR.

36. The Swedish legal framework, does not address the fundamental questions regarding when and how exemptions can be made from the GDPR. On the contrary, it affords MrKoll an exemption to the whole GDPR linked to the mere possession of a certificate of no impediment. This leads to a situation where, MrKoll, who operates in just the same way as a data broker, can "legally" **sell information** that has **nothing to do** with journalism.[27]

37. Consequently, the IMY should question whether Swedish law itself is in line with Article 85 GDPR.[28] In other words, is the loose granting of the certificates, which in turn leads to the blanket exemption protecting MrKoll's business model, really "*necessary*" to protect journalistic purposes, as mandated by Article 85(2) GDPR?

---

[25] Along the same lines, a recent reform proposal: Det kan uttryckas så att journalistikens självklara uppgift i demokratier är att informera, granska och debattera. Angrepp mot journalister, redaktörer och andra som deltar i det offentliga samtalet kan således få konsekvenser inte bara för den enskilda personen utan i förlängningen även för yttrandefriheten och den fria åsiktsbildningen som sådana. Om journalister, redaktörer och andra avstår från att förmedla nyheter, bilda opinion eller annars framföra sina åsikter gällande olika samhällsfrågor av rädsla för att det kan leda till hot eller andra brott kan det i förlängningen försvaga demokratin. Det finns mot denna bakgrund ett starkt intresse av att värna yttrandefriheten och förutsättningarna för journalister och andranyhetsförmedlare att obehindrat delta i den offentliga debatten (Prop. 2022/23:106). See also, Ramsbrodomen (NJA 2001 s. 409)

[26] CJEU, 14.2.2019, *Buividis*, C-345/17, § 66.

[27] In the words of a Swedish citizen, reviewing MrKoll's service: "*There is a special place in hell for companies like this. See, in Sweden the freedom of information as a principle was established to strengthen transparency and accountability. And then there are companies and sites like this one who leech on this regulation just to cash in some low hanging money. It is actually ironic that the mother company, Nusvar AB actually tries to hide all contact information on their abomination of website*." (**Attachment 17**). The author of this review captures, in clear and direct words, the problem of operators like MrKoll and the relevant Swedish legislation that indirectly favours their existence. MrKoll does not operate journalistic activities and consequently does not deserve the protection granted to journalism for the safeguarding of transparency and public interest debate. Supranational and Swedish case law has, moreover, consistently reaffirmed this clear demarcation.

[28] The IMY has already published an analysis of the problem we are dealing with today. It seems evident, from the review of case law carried out in that document, that IMY has already fully framed the issue and provided a solution to the case, in the same terms suggested by the complainant. In particular, reference is made to Swedish case law that excludes

38. Given MrKoll's activites, it is very hard to believe so. The CJEU has clarified that "*the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in* [the GDPR] *must apply only in so far as is* ***strictly necessary*** *(see, to that effect, CJEU, 16.12.2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727,* §56*)*" (emphasis added) (CJEU, 14.2.2019, *Buividis*, C-345/17, § 64).

39. To understand what is "*strictly necessary*", attention should be paid to Article 52 of the Charter of Fundamental Rights of the European Union ("*CFR*"). To be in line with the CFR, any limitation to a fundamental right must fulfil the following four requirements:

i. it must be provided for by law;
ii. it must respect the essence of those rights and freedoms;
iii. it must pursue objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (legitimate aim);
iv. it must, in accordance with the principle of proportionality, be necessary and genuinely meet the aims pursued (principle of proportionality).

40. As to the first point, (i), there is no doubt that the specific limitation on data protection in Sweden is provided for by law (DSL and YGL).

41. The second point of the test, (ii), requires that the Swedish national law respects the "essence" of the right to data protection. A limitation is valid if it restricts the fundamental right in well-defined and limited circumstances.[29] However, in the present case, the situation is quite different. As set out in the preceding paragraphs, the Swedish framework declares the GDPR to be **completely inapplicable** (Article 7 DSL) if there is a "*conflict*" between the GDPR and the YGL. Taking this reasoning to extremes, entities such as MrKoll could - and in fact, can - use the personal data of Swedish residents without any limitations. Even when a Swedish data subject requests the removal of their data, the request is rejected. This is a limitation that excludes the protection of personal data in its entirety and thus, by definition, its "*essence*".[30] If the essence is breached (as in this case), national law is declared contrary to EU Law and an analysis under steps three and four are not required.[31] Nonetheless, as we show below, the Swedish system remains problematic also in third and fourth points.

42. According to point (iii) of the test, the question asked is whether Swedish law serves a general interest objective or the need to protect the rights of third parties (Article 52(1) Charter). On this point, clarity is necessary to avoid a possible misunderstanding. The objective of protecting freedom of expression pursued by the YGL is obviously of general interest. In its practical implementation, however, the law ends up pursuing a "slightly" different objective, which is making MrKoll's business model possible. This permits a parallel database of almost all Swedish citizens for profit and bypasses Swedish authorities who, in theory, should be the ones responsible for the giving out the same information, within the limits of Article 86 GDPR. Such a business model is not

---

from the scope of journalism information of (i) a purely private nature that (ii) in no way contributes to the public debate (**Attachment 18**).

[29] See, for example, CJEU, 13 June 2017, *Eugenia Florescu and Others v. Casa Județeană de Pensii Sibiu and Others [GC]*, C-258/14, § 55; CJEU, 5 July 2017, *Werner Fries v. Lufthansa CityLine GmbH*, C-190/16, §§ 38 and 75; CJEU, 20 March 2018, *Criminal proceedings against Luca Menci* [GC], C-524/15, § 43.

[30] In Schrems I, the CJEU considered that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, did not respect the essence of the right to an effective remedy and to a fair trial, as enshrined in Article 47 of the Charter. See, CJEU, 6.10.2015, *Maximillian Schrems v. Data Protection Commissioner* [GC], C-362/14, § 94.

[31] FRA, Applying the Charter of Fundamental Rights of the European Union in law and policy making at national level, p. 73 (available here). See also, CJEU, 6.10.2015, *Maximillian Schrems v. Data Protection Commissioner* [GC], C-362/14.

a general interest recognised by the Union. In this sense, the problem is not with the entirety of Swedish law, but only with the parts that permit MrKoll's operations. The specific reference is, therefore, to Article 1:4 and 1:5 YGL.

43. Finally, the fourth point of the test (iv), requires an examination of whether the measures taken at the national level are "appropriate" to the purpose.[32] Measures are appropriate when they are suitable to guarantee the result in a consistent and systematic manner.[33] This is certainly not the Swedish case. The national framework, formally inspired by freedom of expression and information, in practice allows almost any economic operator to obtain a license of no impediment. This, in turn, leads to an almost total exemption from all GDPR. This is too exorbitant a limit on the right to data protection under Article 8 CFR. Less intrusive choices on such a right would, in fact, be possible.[34] When there is a choice between several appropriate measures, national laws must adopt the least onerous, that is, the measure that interferes least with the fundamental right to data protection.[35] Swedish law does not respect this requirement and is not proportionate to the aim pursued. With the intention of protecting freedom of expression from unlawful interference, YGL ends up guaranteeing MrKoll the ability to act in an **uncontrolled manner**. Furthermore, the disadvantages are absolutely disproportionate. To give just a few examples, MrKoll is used by stalkers and ex-partners to follow and harass women. Recently, the service was reportedly used by rival gangs to know the geographical location of their opponents. The bombs and attacks also did not spare innocent lives, such as the young 24-year-old Soha Saad, who was killed by mistake by the detonation of the explosives.[36]

44. As a consequence, only one conclusion remains. The articles of the YGL that allow MrKoll to operate in this way are contrary to the EU Charter of Fundamental Rights and the GDPR. They must therefore be disapplied by virtue of the principle of primacy of EU law.

45. On this point, the Court of Justice has already held that the duty to disapply national legislation that contravenes EU law is not only incumbent on the national courts but also on the national supervisory authorities called upon to apply European legislation, in this case the GDPR. In these precise terms: "*The duty to disapply national legislation which contravenes Community law* ***applies not only to national courts but also to all organs of the State, including administrative authorities*** *(see, to that effect, Case 103/88 Fratelli Costanzo [1989] ECR 1839,* §31*), which entails, if the circumstances so require, the obligation to take all appropriate measures to enable Community law to be fully applied) and (Case 48/71 Commission v Italy [1972] ECR 527, paragraph 7)*. See also (CJEU, 9.9.2003, *Consorzio Industrie Fiammiferi (CIF) v Autorità Garante della Concorrenza e del Mercato*, C-198/01, §49)". Along the same line and more recently, (CJEU, 14.09.2017, *The Trustees of the BT Pension,* C-628/15, § 54), and (CJEU, 04.12.2018, *The Minister for Justice and Equality and The Commissioner of the Garda Síochána v Workplace Relations Commission*, C-378/17, §38).

---

[32] The purpose of the YGL law is to protect freedom of expression (Article 1 YGL).
[33] CJEU, C-190/16, 5 July 2017, *Werner Fries v. Lufthansa CityLine GmbH*, § 48.
[34] For example, "journalism" may be exempted from Article 6(1) GDPR. Or perhaps, in order to protect journalistic sources, it could enjoy, among the others, an exemption from Article 15(1)(g) GDPR ("*any available information as to their source*"). However, certain rights must still be guaranteed. For example, online newspapers and magazines, are often required to respect the right to rectification under Article 16 GDPR. Sometimes, also to the deletion of data, if the subject matter is not in the public interest.
[35] CJEU, 20.5.2003, Österreichischer Rundfunk, Joined Cases C-465/00, C-138/01 and C-139/01, §102. See also, CJEU, 30 June 2016, *Lidl GmbH & Co. KG v. Freistaat Sachsen*, C-134/15, § 33; CJEU, 12 July 2001, *H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren and Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren v. Minister van Landbouw, Natuurbeheer en Visserij*, C-189/01, § 81.
[36] The Guardian, 11.2.2024, *'People are scared': Sweden's freedom of information laws lead to wave of deadly bombings* (available here) (last accessed, 12.2.2024).

46. The constitutional nature of Article 1:4 and 1:5 YGL in no way affects this conclusion. In CJEU, 03.06.1964, *Costa v ENEL*, C-6/64, the Court of Justice built on the principle of direct effect and captured the idea that the aims of the treaties would be undermined if EU law could be made subordinate to national law. As the Member States transferred certain powers to the EU, they limited their sovereign rights, and thus in order for EU norms to be effective they must take precedence over any provision of national law, **including member state constitutions**.[37] Consequently, the provision of the YGL must be interpreted in conformity with the EU rules or, more likely, disapplied in the parts that are incompatible with the GDPR.

47. Hence, **the IMY must disapply the Swedish legislation** when it provides that a data controller such as MrKoll (who does not exclusively or predominantly engage in journalistic activities) nevertheless benefits from the protection afforded to journalism. In particular, the IMY should verify that the holder of a certificate of use pursuant to Article 1:4 YGL, only engages in journalistic activities when processing personal data under these exemptions. If the holder cannot prove this, then the IMY should disapply Article 1:4(d) YGL, as it is in direct violation of EU law and Article 85(2) GDPR. Accordingly, the GDPR would subsequently become applicable in its entirety against MrKoll.

3.2.2 Swedish law limits the protections to sensitive data, thereby providing for an unreasonably wide derogation from EU law

48. A second problem concerns the concrete balancing between freedom of expression and data protection in Article 1:20 YGL. This provision limits freedom of expression, but only when special categories of personal data are involved and other requirements are met (§§ 25-27 above). In doing so, Swedish law introduces a derogation to the scope of EU law and the GDPR. Again, this derogation must be strictly necessary (§ 37) and thus comply with the proportionality test required by Article 52(1) CFR.

49. In the present case, the measure does not appear to be appropriate. The fact that the GDPR provides reinforced protection for the categories of data referred to in Article 9 GDPR, does not mean that other types of data do not deserve protection. Far from it. The processing of "non-sensitive" personal data can result in infringements of individual liberties that are sometimes far more serious than those associated with the processing of sensitive data.

50. To give a few examples. The publication of an individual's criminal record makes it possible to infer very important aspects with respect to his or her mental health. The first and last name and date of birth of a minor, published in the motivation part of such records, do not constitute sensitive data, yet they expose the minor to extremely serious risks. The combination of an individual's age, together with the geographical location of his or her home or the model of the cars he or she owns certainly do not concern health data. Yet they can lead malicious individuals to orchestrate a robbery or theft. Informing the rest of the Swedish population about a certain individual's co-habitants is not data protected by Article 1:20 YGL. Yet, if one of the housemates gets involved in a racially motivated series of murders, the "domestic" proximity may - wrongly - suggest the political affiliation of the housemates. In short, there is no clear separation between "special categories of data" and "ordinary" data. The GDPR is clear on this point: all personal data must be protected, sometimes some more strongly than others.

[37] Further examples of cases in which the Court affirmed the primacy of EU law include: CJEU, 12.12.1970 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle fur Getreide und Futtermittel*, C11/70; CJEU, 09.03.1978, *Amministrazione delle Finanze dello Stato v Simmenthal SpA*, C-106/77; and CJEU, 13.11.1990, *Marleasing SA v La Comercial Internacional de Alimentacion SA,* C-106/89.

51. Swedish law does not consider these possibilities. Through Article 1:20 YGL, it just limits the protection of Swedish citizens and residents to the protection of (some) special categories of data, unreasonably sacrificing other "non-sensitive" data on the altar of freedom of expression. In fact, an exception to the GDPR is introduced that is unnecessary and in open violation of European law.[38] On this condition, Swedish law and Article 1:20 YGL stands in clear opposition to the GDPR, creating a clear problem of compatibility with European law.

52. In relation to the IMY's obligation to intervene directly, see § 45 above.

53. The "constitutional" nature of Article 1:20 YGL in no way affects this conclusion. See, § 46 above.

54. In these terms, IMY should disapply the first paragraph of Article 1:20 YGL, insofar as it limits the scope of the exemption to special categories of data. By doing so, the GDPR would come back into full application, also in relation to the data processed by MrKoll, bringing the entire Swedish system back in line with European law.

3.3 The GDPR is therefore fully applicable to MrKoll

55. Because of the above, the IMY must either interpret national law in a manner consistent with EU law or directly disapply national law that is contrary to EU law. Consequently, declaring the GDPR applicable and finding that MrKoll has committed at least the following violations.

4. VIOLATIONS

4 .1 Violation of Article 14 GDPR

56. MrKoll does not provide Swedish residents with the information required by Article 14 GDPR.

57. Under Article 14 GDPR, after acquiring the user's personal data, the controller should inform the data subject about the processing. MrKoll should at least have published the information on its website pursuant to Article 14(5)(b) GDPR. This form of communication never took place. In fact, MrKoll doesn't even have a privacy policy as they consider themselves exempted from the GDPR.

58. No information under Article 13 GDPR is ever provided either.

4.2 Violation of Article 6(1) GDPR

59. MrKoll does not provide any information on its processing (§ 56-58 above), therefore it is not possible to know the legal basis it relies upon under Article 6(1) GDPR.[39] In any case, MrKoll carries out as a controller different processing operations, all of which are nevertheless relevant under Article 4(2) GDPR. We can distinguish these operations into three distinct categories:

---

[38] The CJEU has clarified that " *the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in [the GDPR] must apply only in so far as is strictly necessary (see, to that effect, judgment of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C 73/07, EU:C:2008:727, paragraph 56*)" (CJEU, 14.2.2019, *Buividis*, C-345/17, § 64).

[39] Under Articles 5(2) and 14 GDPR, it is for the controller to provide such information. If that does not occur, the processing must be declared unlawful and stopped.

60. The first concerns the phase of **obtaining data** from Swedish public authorities and storing it into MrKoll's systems. In this sense, we imagine that MrKoll requests the public administration, directly or indirectly,[40] to obtain the personal data of Swedish citizens and residents.

61. Once the data is received, MrKoll **organises, structures, consults, connects and uses** the information, so that it is easily searchable and retrievable.

62. Finally, the third phase involves the **dissemination** through transmission or making available of the previously organised personal information to users of the website.

63. Obviously, all such operations must be justified and based on a relevant legal basis within the meaning of Article 6(1) GDPR. However, even if one were to assume an Article 6(1) GDPR legal basis under which MrKoll could hypothetically operate, none can be found.

64. To begin with, the data subject has never given any consent to the processing of his data (Article 6(1)(a) GDPR), let alone ever signed any contract with the controller (Article 6(1)(b) GDPR). The processing is certainly not imposed on MrKoll by any legal obligation (Article 6(1)(c) GDPR) nor is it necessary to protect the vital interests of the data subject (Article 6(1)(d) GDPR) or perform a task in the public interest (Article 6(1)(e) GDPR).

65. The controller also cannot rely on the last legal basis, legitimate interests referred to in Article 6(1)(f) GDPR. The CJEU has already held, that Article 6(1)(f) GDPR lays down three cumulative conditions so that the processing of personal data covered by that provision is lawful. First, the pursuit of a **legitimate interest** by the data controller or by a third party. Second, **the need to process personal data for the purposes of** the legitimate interests pursued. Third, that the interests or fundamental freedoms and rights of the person concerned by the data **protection do not take precedence** over the legitimate interest of the controller or of a third party (CJEU, 17. 6.2021, *M.I.C.M.*, C-597/19, § 106).

66. **First,** we doubt that MrKoll's initial acquisition of the data is even legitimate (§ 60). MrKoll's entire activity is essentially based on a massive scraping of Swedish public databases.[41] The company does not - nor could it, given the nature of the business - declare any specific interest in obtaining the data from the Swedish public authorities. The massive acquisition of personal data is based solely on a misinterpretation of the principle of access to public databases typical of the open Swedish institutions. The transfer of data from "public" to "private" has recently been declared unlawful by the Court of Justice, especially in the presence of confidential data and in the

---

[40] On its website, MrKoll in fact claims to collect the information from public databases. One of these is called SPAR. The personal data of the complainant held by SPAR (**Attachment 19**) are curiously overlapping with those held by MrKoll (See, *Attachment 14*). It can therefore be reasonably assumed that MrKoll receives the data from SPAR for marketing purposes, at least indirectly. We say "*indirectly*" because, according to the response provided by SPAR following an Article 15 GDPR access request (see *Attachment 20*), MrKoll is not among the recipients of SPAR's data. Among them, however, is another famous data broker, *Dun and Bradstreet*. The data subject requested the latter to provide a specific indication of the recipients, in order to verify that the latter had in turn provided personal data to MrKoll for the latter's publication. *Dan and Bradstreet,* however, rejected the request to obtain the specific recipients on the ground that it was not obliged to indicate them. This, of course, in open violation of the recent CJEU, 12.01.2023, *Österreichische Post AG*, C-154/21 which, on the contrary, requires the controller to provide such specific indication when requested by the data subject, as was the case here (**Attachment 20**).

[41] Interestingly, while selling information for a fee, MrKoll prohibits its users, through its Terms of Service, from creating personal archives or researching information about individuals. Which seems strange, to say the least, given the company's slogan: "Better control over private individuals". Furthermore, the same terms, make it clear that the "information" is intended exclusively for the customer and may not be further published or shared publicly. Once again, it seems that the company contradicts its own reason for existing. In other words, the only one authorised to profit from the Swedish institutions' principle of transparency is only MrKoll.

absence of a specific interest of the applicant in obtaining it. Exactly, the case of MrKoll: "*Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as* ***precluding national legislation*** [...] *which authorises a public body to disclose data of that kind to economic operators in order for the data to be re-used and disclosed to the public by them*" (emphasis added) (CJEU, 22.6.2021, Case C-439/19, *B v. Latvijas Republikas Saeima*, §125). In other words, **MrKoll's business model is flawed at its base**. Obtaining the data from Swedish institutions without a specific interest is **already** in breach of the GDPR. The same argument can be made for the next two stages of the processing, namely the internal organisation of the information (§ 61) and, above all, its dissemination to the public (§ 62). The IMY will probably have to use its investigative powers to verify the existence of any kind of legitimate interest with respect to such operations. In any case, it seems rather unlikely that the processing of personal data for the purpose of sale is what the drafters of Article 6(1)(f) GDPR intended.
67.

68. **Second**, following the Court's instructions, we need to determine whether MrKoll's activity is "necessary" to pursue the (questionable) purposes mentioned above. It is quite obvious that no such necessity exists. Take the first "phase" of MrKoll's activity – obtaining the data from Swedish authorities (§ 60). No one prohibits MrKoll from helping a certain individual find information about another. Such activity, however, should be done in a manner consistent with the principle of data minimization (Article 5(1)(c) GDPR). For example, once the specific interest of the requester has been assessed, MrKoll could interact with Swedish authorities to obtain the requested information. But this would be a specific request, motivated by a specific interest. Not a bulk acquisition of data of all sorts as is the case now. In other words, the purpose of "informing" does not justify the creation of a parallel database of the entire Swedish population including the selling of confidential personal information and judicial records. In its recent decision SCHUFA, the Court of Justice has clearly confirmed the above: "*there are* ***doubts*** *as to the lawfulness of a private agency such as SCHUFA storing data transferred from public registers in its own databases. First of all,* ***that storage does not take place in relation to a specific reason****, but rather in the* ***event*** *that their contractual partners ask them for such information* [...] *In this case, only the condition set out in point (f) of the first subparagraph of Article 6(1) of the GDPR is relevant.* ***It is doubtful*** *whether a credit information agency such as SCHUFA is pursuing a legitimate interest within the meaning of that provision*" (emphasis added) (CJEU, 7.12.2023, *SCHUFA Holding AG*, Joined Cases C-26/22 and C-64/22, §§).[42]

69. Finally, **third**, it must be determined that the interests and freedoms of the data subject do not override the (questionable [§ 67] and disproportionate [§ 68]) interests of the controller. On this point, the CJEU has recently clarified that, when balancing the interests of the controller and those of the data subject, special consideration must be given to the *"reasonable expectations of the data subject"* as well as to the *"particularly extensive"* nature of the data processing under consideration (CJEU, 4.7.2023, *Bundeskartellamt*, C-252/21, §§ 117-118). The controller admits that the data it holds and publishes comes from Swedish public databases (§ 4 above). When the complainant goes to the Tax Authority (or any other public authority from which MrKoll acquires personal information) and discloses his new address, phone number, or VAT number, it is because he is expected to keep his details up to date under Swedish national law. He does not reasonably expect MrKoll to then acquire this information and create an accessible and detailed profile of his life. After all, he his disclosing his data due to a legal obligation not because he expects somebody

[42] In line with the SCHUFA decision, among the many, also CJEU *Asociația de Proprietari bloc M5A-ScaraA,* which focuses on the data minimization principle: *"the need for processing must be examined in conjunction with the 'data minimisation' principle enshrined in Article 5(1)(c) of the GDPR, in accordance with which personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"* (CJEU, 11.12.2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, § 48).

else to sell it onwards. Even if this would be the case, the processing would be drastically disproportionate in favour of the controller and therefore, once again, unlawful.

70. In conclusion, MrKoll's processing has no legal basis under Article 6 GDPR and is therefore radically unlawful.

4.3 Violation of Article 17 GDPR

71. As explained above, the complainant requested the controller, pursuant to Article 17 GDPR, to delete his personal data from the platform. This included, among others, first name, last name, residential address and information related to his economic activity. The controller refused the request, claiming that the GDPR did not apply and that therefore the data subject could not claim the erasure of his data (§16 of this complaint). Since, on the contrary, the GDPR applies to the controller's activity (§§ 30-55 above), this position has no legal basis and the controller's refusal to act is unlawful for the following reasons.

4.3.1 Article 17(1)(d): personal data have been unlawfully processed

72. As explained above, MrKoll's activities do not appear to be covered by any legal basis under Article 6(1) GDPR (see, §§ 59-69 above). IMY must therefore find that the processing is radically unlawful and, accordingly, order the deletion of all personal data of the complainant pursuant to Article 17(1)(d) GDPR.

4.3.2 Article 17(1)(c): the claimant objected to the processing under Article 21 GDPR

73. As anticipated, it is not possible to know the legal basis used by MrKoll to sell the data of millions of Swedish residents online. Assuming that Article 6(1)(f) is the legal basis used by the controller, it can therefore be argued that the data subject's request was made under Article 17(1)(c) of the GDPR.Since MrKoll does not inform on its processing, the claimant objected to the processing of his data under Article 21(1) GDPR. There is no demonstration of any overriding interest of MrKoll in the publication of the data following the request for deletion. In its response, the company simply states that the GDPR does not apply to its operations. It is indeed difficult to imagine that a platform that profits from the sale of personal data would have a protected interest overriding the privacy expectations of the data subject. To give just one example, the data published by MrKoll is used by abusive ex-partners to stalk former partners, a very significant issue in the field of violence against women. Women who, despite changing address or telephone number, are still easily traced by their stalker (**Attachment 21**).[43] It is hard to believe that the controller could justify an overriding interest (see § 56 above) to publish personal details when it has this type of societal impact.

4.3.3 Article 17(1)(b): No consent was ever given

74. The complainant (nor any other Swedish resident) has ever given their consent to the processing and publication of their data on MrKoll's website.[44] Article 17(1)(b) GDPR, therefore, does not apply to the present case.

---

[43] Another review on MrKoll that can be found online: "Awful dodgy *company. Awful dodgy company, it doesn't allow you to hide birthday, age, phone number or address like other websites. I want privacy for my information and have to deal with a* ***stalker*** *because of this s*** dishonest website.*" (emphasis added).

[44] From an online review of the service*: "Personal information published for whole world without my consent. Please, report it to Google and to other applicable EU-authorities as Swe-authorities will not lift a finger. Hope that this site will be banned and owners prosecuted*." Another one: "*Very bad page, no one even asked me for any permission if I want to spread all my personal information on google in this page. And they don't respect my request that I don't want to show any*

4.3.4 Article 17(1)(e): Swedish law should be disapplied

75. The same conclusion must be reached for the other case envisaged by Article 17 GDPR. Due to the inapplicability of the Swedish GDPR exemption rules (Article 7:1 DSL), the data must be deleted for "*compliance with a legal obligation in Union* [...] *law*" (Article 17 GDPR itself, in this case).

4.3.5 No exemptions under Article 17(3) GDPR

76. Also, none of the exemptions in Article 17(3) GDPR are applicable to the present case. Notably, due to the above, MrKoll's processing is not necessary to exercise the right to freedom of expression and information as allowed by Article 85(2) GDPR.

77. Hence, by not deleting the complainant's personal data after it was requested, the controller breaches Article 17 GDPR.

4.4 Violation of Article 10 GDPR

78. The above analysis also shows a clear violation of Article 10 GDPR. MrKoll allows anyone, by payment of a small sum of money, access to the full list of criminal and judicial records of Swedish citizens (see §10 above, fn. no. 1). By doing so, it processes personal data relating to criminal convictions and offences which, under Article 10 GDPR, may only be carried out by public authorities.

79. Swedish law, does not - nor could it, given the primacy of EU law - authorise MrKoll to process such data, and does not provide "*appropriate safeguards for the rights and freedoms of the data subject*", as expressly required by Article 10 GDPR. In any event, MrKoll provides the criminal and civil convictions of virtually all Swedish citizens. This is a "*comprehensive register of criminal records*" that can be maintained "***only** under the control of official authority*" (emphasis added). Control which, in this case, is non-existent. Consequently, a violation of Article 10 GDPR is evident.

80. Among other things, the Court of Justice recently recalled that where publication entails the effect of disapproval and social stigma attached to certain conduct, especially if of criminal relevance, neither sharing nor publication is permitted, especially in the absence of a **specific interest** shown by the applicant. In particular, "*Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish **a specific interest** in obtaining the data. (§125). Those provisions must, for reasons identical to those set out in the answer to the second question, be interpreted as also **precluding national legislation which authorises a public body to disclose data of that kind to economic operators in order for the data to be re-used and disclosed to the public by them***' (CJEU, 22.06.2021,*B v. Latvijas Republikas Saeima*, C-439/19, §125) (emphasis added)

81. The argument above is important, not only to protect the convicted person's right to data protection and privacy but also, to limit the collateral victims. For example, the convictions relating to the Swedish woman (cited above as Ms A) concerned conduct involving violence, alcohol and domestic abuse with the involvement of minors and with indication of the full name and date

---

informations because I have my own reasons. Why you don't respect my privacy???????? You don't have the right to do that."

of birth of those minors. Minors who, in turn, could be traced in the future by anyone who might intend to profit from such traumas. The same is to be said for the Linder family, who found themselves at the top of the most consulted profiles on MrKoll, simply for living at the same address as a person accused of a racially motivated attack.

82. Consequently, the processing of personal data relating to criminal convictions or the like must be considered explicitly contrary to Article 10 GDPR.

5. APPLICATIONS

83. The situation reported on the previous pages gives cause for great concern. In Sweden, there is a general non-application of the GDPR by MrKoll and similar operators. A considerable amount of data, sensitive and non-sensitive, is published without any consent from or information provided to the complainant and Swedish citizens. On many occasions, such data is used to perpetrate violence against women and individuals completely unrelated to journalistic purposes. Not even children are spared. It is therefore necessary for IMY to take a clear and swift stand in relation to this unacceptable state of affairs.

5.1 Request to investigate

84. The complainant hereby requests that the competent supervisory authority fully investigate the complaint using the powers granted to them under Article 58(1) GDPR.

5.2 Request to adopt specific corrective measures

85. As foreseen in Article 58(2)(c) GDPR, the complainant requests that the competent supervisory authority order the controller to comply with the claimant's erasure request under Article 17 GDPR and, according to Article 58(2)(g) GDPR, to remove all his personal data from its servers and IT systems.

86. Pursuant to Article 58(2)(g) GDPR, the complainant requests that the controller notifies any recipients of his or her personal data of the deletion of data pursuant to Article 17(1) and (2) GDPR, requiring them to proceed with the deletion of personal data by any means, unless justified by another legal basis.

87. In view of the radical unlawfulness of the processing carried out by the controller, the complainant also requests, pursuant to Article 58(2)(f) GDPR, to order the absolute prohibition of any further processing of data concerning him on its servers and any other IT system in its possession.

5.3 *Procedural notes*

88. The complainant, in view of the gravity of the alleged violations, calls upon the IMY for a prompt decision of the complaint. To this end, it must be noted that the requests developed above (§§ 85-87 above) concern a specific subjective right of the complainant (Article 17 GDPR). With respect to such requests, should the IMY adhere to the complainant's position, there is no administrative discretion, and they must be granted according to the timeframe established by Swedish administrative law. In light of this, the complainant respectfully anticipates that, in the event that a decision on the aforementioned points is not reached within the statutory time limit (6 months from the filing of this complaint, §12 of Swedish Administrative Law (2017:900), the complainant will exercise the right to request a decision as provided for by Swedish administrative law and, if necessary, refer the matter to the Stockholm Court for a further decision.

6. OTHER

89. Communications between *noyb* and the supervisory authority in the course of this procedure can be done via email at [redacted] with reference to the Case-No C-077 (also mentioned in the title of this complaint).

Signature

Stefano Rossetti Max Schrems