To the President and Members of the
GENERAL COURT OF THE EUROPEAN UNION

APPLICATION

Action for damages pursuant to art. 268 and art. 340, second paragraph of the Treaty on the Functioning of the European Union

on behalf of

Mr Frank van der Linde,
Address: Linnaeusstraat 2A, 1092 CK, Amsterdam, the Netherlands
(Note: Although the Applicant resides in Amsterdam, the Netherlands, he has no permanent residential address, reason why, as instructed by the Registry of the General Court, the address of Applicant's law firm is stated.)

Applicant,

represented by Mr Thomas van der Sommen and Mr Emiel Jurjens, attorneys-at-law working for the law firm *Prakken d'Oliveira Human Rights Lawyers*, based in Amsterdam, (address: Linnaeusstraat 2A, 1092 CK, Amsterdam, the Netherlands) who agree, for the purpose of these proceedings that all procedural documents be lodged and served via e-Curia in accordance with art. 56a(1) Rules of Procedure of the General Court,

v

European Union Agency for Law Enforcement Cooperation (Europol),
Address: Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands

Defendant,

FOR:

- compensation for damage which Van der Linde has suffered as a result of the unlawful acts and omissions by Europol, as specified below.

Amsterdam, 9 October 2025

Representation

In accordance with art. 51(2) Rules of Procedure a certificate has been lodged proving that Mr E.W. Jurjens is a member of the Amsterdam Bar Association and therefore authorised to practice and represent Van der Linde before the General Court. For Mr T.J.R. van der Sommen this certificate has already been lodged for the purposes of opening an account giving access to e-Curia.

TABLE OF CONTENTS

I. INTRODUCTION

1. This Action for damages under art. 268 jo art. 340(2) TFEU is brought because the European Union Agency for Law Enforcement Cooperation (**Europol**) breached its obligations in respect to and violated the rights of Mr Frank van der Linde (**Van der Linde**), which caused him damage. Van der Linde has been wrongfully associated with terrorism in a message from the Dutch Police to Europol, and possibly others. This message has been unlawfully processed by Europol and was included in its systems associating Van der Linde with terrorism. A data access request on this matter by Van der Linde has been completely mishandled by Europol. Europol did so by falsely stating that it did not have personal data to which he could get access, while in fact Europol was aware it had at least two items of personal data of him since it secretly conspired with others resulting in Europol deleting his personal data. Moreover, Europol frustrated a subsequent investigation of the European Data Protection Supervisor (**EDPS**) into Van der Linde's case. This did not prevent the EDPS from concluding that Europol acted unlawfully and discovering that Europol, contrary to its claims, did actually still had access to his personal data.

2. Europol is a body of the European Union pursuant to art. 1 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (**Europol Regulation** or **ER**).[1] Europol incurred non-contractual liability for the damage suffered by Van der Linde as set out in arts. 49(3) and 50(1) ER. It did so by failing to comply with its obligations under arts. 18(1), 18(2), 28(1), 30(2), 30(3), 31(1), 31(6), 36(1), 36(2), 36(4), 36(5), 36(6), 36(7), 37(1), 38(3), 38(4) and 40(1) ER and arts. 7, 8(1), 8(2), 41(1), 41(2) and 47 Charter of Fundamental Rights of the European Union (**EU Charter**).[2] Thereby it infringed the right to respect for private and family life, the right to the protection of personal data, the right of access to personal information, the right to rectification and erasure, the right to good administration and right to an effective remedy. Europol did so by (i) failing to assess that the processing of Van der Linde's personal data was in accordance with Europol's objectives, i.e. whether it acted within its legal mandate, and also by processing Van der Linde's personal data in breach of Europol's obligations, and (ii) the subsequent failure of Europol to adequately handle the request of access to personal data submitted by Van der Linde. The law applicable to the Europol's conduct and omissions at the material time is the Europol Regulation, which entered into force on 13 June 2016, and was only amended in 2022 by Regulation (EU) 2022/991 of 8 June 2022.

3. In this Action for damages, Van der Linde will first set out that he complies with the requirements of admissibility (chapter 2). Then the facts will be set out (chapter 3). Chapter 4 sets out the legal framework. In chapter 5 the unlawful conduct of Europol is detailed by setting out the legal obligations it violated. Together with the pleas I-VI, Van der Linde will substantiate that the rules of law breached by Europol confer rights on individuals like him and that the conduct of Europol resulted in sufficiently

---

1 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135/53.

2 Charter of Fundamental Rights of the European Union, 7 June 2016, OJ C 202/391.

serious breaches of rules of law. Van der Linde will then specify the damage suffered (chapter 6), as well as the causal link between Europol's unlawful conduct and the damages incurred by Van der Linde (chapter 7). In the final chapter, Van der Linde will set out his conclusions and the orders sought (chapter 8).

II. ADMISSIBILITY

4. This Action for damages is admissible. Van der Linde sent a notice of liability to Europol requesting compensation of his damage on 10 June 2025 (**Annex A.1**).[3] This was within the five year limitation period for matters arising from non-contractual liability as he first came to the knowledge that Europol potentially acted wrongfully against him on 11 June 2020, the date Europol rejected his request to access his personal data. Subsequently, Van der Linde instituted proceedings before the General Court of the EU on 9 October 2025, which is within the four month (two times two) time limit, as Europol did not respond to Van der Linde's application within two months and thus implicitly rejected his application. Therewith, Van der Linde complies with art. 46 Statute of the CJEU.

5. Van der Linde suffered actual and certain damage. The damage is a direct result of the unlawful conduct of Europol. That conduct constitutes as a sufficiently serious breach of the above-mentioned obligations that confer rights on individuals, i.e. Van der Linde, resulting in the violation of his fundamental rights under arts. 7, 8, 41 and 47 EU Charter and arts. 36 and 37 ER. Furthermore, the unlawful conduct by Europol in and of themselves qualifies as a breach of arts. 7, 8, 41 and 47 EU Charter. The requirements for admissibility of this Action are fulfilled.

III. FACTS

III.1 Introduction

6. Van der Linde is a Dutch citizen, and he worked as a management consultant and the director of Fairfood, a Dutch NGO. He engages regularly in the peaceful exercise of his rights to freedom of expression and freedom to protest on issues of public interest and is an outspoken peaceful activist.

7. Van der Linde has been wrongly and unlawfully designated as a leftwing extremist and associated with terrorism by, as far as he knows, the Dutch police, the Dutch National Coordinator for Security and Counterterrorism (**NCTV**) and the Municipality of Amsterdam. As a consequence, the Dutch authorities imposed far reaching and mostly secret measures that drastically infringed on his fundamental rights. This severely and negatively impacted his life for the past 11 years in multiple ways and caused a great deal of damage. Van der Linde gradually uncovered (the scope of) these violations and repressive measures through personal data requests and freedom of information requests. Subsequently, he embarked on a quest to seek access to his personal file to uncover the full extent of his unlawful treatment. In this process Van der Linde discovered that the Dutch police had shared information with Europol.

---

[3] Letter Van der Linde to Europol re. notice of liability, 10 June 2025 (**Annex A.1**).

8. After further investigation Van der Linde found that Europol had processed sensitive personal data of him unlawfully. The EDPS concluded after its own investigation that Europol had breached the Europol Regulation and the EU Charter *(inter alia* art. 36(6) ER, read in conjunction with art. 41 EU Charter, and arts. 36(1), 36(2) and 36(5) ER). It concluded that Europol insufficiently motivated its decision to reject Van der Linde's data access request, wrongly referred part of Van der Linde's request to the Dutch Police, failed to provide all information and potentially wrongfully deleted information (**Annex A.2**).[4]

9. In the subsequent sections of this chapter the facts are presented regarding the unlawful actions of the Dutch authorities against Van der Linde (section III.2), background on Europol and the data subject access request of Van der Linde to Europol (section III.3), the decision of the EDPS on Van der Linde's complaint against Europol (section III.4) and the ongoing cases before the EDPS and the District Court of Amsterdam (section III.5).

III.2 Unlawful actions Dutch authorities against Van der Linde

III.2.1 Background

10. As mentioned, Van der Linde regularly exercises his right to freedom of expression and his right to protest to stand up for matters of public interest, such as anti-discrimination and climate change. Over the last 9 years Van der Linde has gradually found out that the Dutch authorities covertly monitored him, stored his personal data and shared his data with national and international law enforcement and intelligence agencies. As a rule, Van der Linde was not informed by the authorities of the far-reaching actions they took in relation to his data. As such, he has mostly been unaware of which pieces of his personal data were shared, with who and under what qualification. Often, Van der Linde only found out that this data has been stored and shared when he either felt the consequences of this (such as being handcuffed and taken away by police during peaceful protests), or, accidentally, through data access requests on other issues (through which he for example found out the reason for why he was questioned at airport security or that the police tried to recruit informants among his friends and contacts) or after legal intervention.

11. In any case, the Municipality of Amsterdam, the Dutch National Coordinator for Security and Counterterrorism and the Dutch Police have been involved in these actions. For each of these authorities it has been established, either by themselves or by the Dutch courts, that they have stored and shared Van der Linde's personal data unlawfully and/or that they have wrongly associated him with terrorism, extremism or radicalization.

12. In all of these cases, it has been incredibly difficult for Van der Linde to get a complete picture of the nature and extent of the unlawful processing of his sensitive personal data. Authorities have (partially) refused Van der Linde access to this information or simply stated they did not store or share his data. He has time and again proved them

[4] Decision EDPS, 8 September 2022, pars. 3.19-3.21, 3.23-3.29, 3.31-3.32, 3.58-3.60 (**Annex A.2**). Van der Linde only possess a partly redacted version of the decision.

wrong, showing repeatedly that data was incorrectly not shared with him and that data which was shared with him was incomplete.

III.2.2 Municipality of Amsterdam

13. Despite repeated advice not to do so from the Police and the public prosecutor's office, in 2017 the Municipality of Amsterdam included Van der Linde in a register of 'persons of interest' in the context of its policy against radicalization (**Annexes A.3 and A.4**).[5] This far-reaching decision resulted in him being personally monitored by the police and his personal data being shared widely among national and international authorities in the context of terrorism. Up until May 2023, the Municipality of Amsterdam defended this decision.

14. However, after continuing efforts by Van der Linde and a police whistle-blower which triggered significant media attention about the matter (**Annex A.5**),[6] on 25 May 2023 the Mayor of Amsterdam sent a personal letter to Van der Linde acknowledging on behalf of the Municipality that he should never have been included in the anti-radicalization policy.[7] The Municipality of Amsterdam was forced to concede that Van der Linde had never met the criteria for inclusion in this policy, noting that "the threat you were perceived to present was insufficiently supported by facts" ("*de dreiging die van u uit zou gaan onvoldoende door feiten wordt ondersteund*").[8] In addition, the Municipality of Amsterdam acknowledged that Van der Linde's right of access to information about the processing of his personal data had been violated as the Municipality had failed to provide him with his complete case file and appointed an expert to ensure he would receive his entire case file.

15. The Municipality of Amsterdam acknowledged that Van der Linde had seriously suffered as a result of its actions, offered its apologies and opened a discussion about compensation for the damage he suffered. In addition, the Municipality of Amsterdam acknowledged structural shortcomings in its policy that came to light as a result of this matter and stated that as a result of this case it has made adjustments to its policies.[9]

III.2.3 National Coordinator for Security and Counterterrorism (NCTV)

16. In the period 2016-2017, the NCTV shared personal data of Van der Linde in at least two instances with national and international security and intelligence authorities, unlawfully associating him with extremism.

---

5 Letter Mayor of Amsterdam to Van der Linde re. unlawfulness inclusion deradicalisation program, 25 May 2023 (**Annex A.3**); News article B. Soetenhorst, 'Lastpak Frank van der Linde belandde in de aanpak radicalisering: 'Heb me extreem eenzaam gevoeld', *Het Parool,* 29 April 2023 (**Annex A.4**).

6 News article B. Soetenhorst, 'Interview Hoe de politie zich ontdeed van een dissidente agent', *Het Parool,* 23 September 2023 (**Annex A.5**).

7 Letter Mayor of Amsterdam to Van der Linde re. unlawfulness inclusion deradicalisation program, 25 May 2023 (**Annex A.3**).

8 Letter Mayor of Amsterdam to Van der Linde re. unlawfulness inclusion deradicalisation program, 25 May 2023, p. 2 (**Annex A.3**).

9 Letter Mayor of Amsterdam to Van der Linde re. unlawfulness inclusion deradicalisation program, 25 May 2023, p. 2 (**Annex A.3**).

17. The Minister of Justice and Safety decided, many years later, that the NCTV was not allowed to include the qualification of "extreme left" ("*extreemlinks"*) in two of its messages about Van der Linde and that the NCTV should not have sent these messages to other agencies (**Annex A.6**).[10] Furthermore, the District Court of Amsterdam concluded that the processing and sharing of Van der Linde's data by the NCTV was unlawful and violated the General Data Protection Regulation (**GDPR**)(**Annex A.7**).[11]

18. In a recent letter to Van der Linde, the Minister confirmed (again) that NCTV should not have used the qualification "extreme left" ("*extreemlinks"*) in two analyses of him, that these should not have been shared with third parties and that this violated the GDPR (**Annex A.8**).[12] The Minister also offered Van der Linde minimal compensation for the damages he has suffered because of this qualification and for spreading his data.[13] Negotiations on this are ongoing.

19. Finally, the Dutch Data Protection Authority (**DDPA**) found that the NCTV violated the GDPR by failing to inform Van der Linde of the processing of his personal data and also found a violation of the obligation under the GDPR to demonstrate compliance (**Annex A.9**).[14]

III.2.4 Police

20. Over the past years Van der Linde has also tried to obtain a full picture of the way the Dutch Police (**Police**) has processed his personal data. In 2017, Van der Linde temporarily moved to Berlin to receive medical treatment. The Dutch authorities knew this, and without his knowledge, the Police informed the German police (the Bundeskriminalamt, **BKA**) about his stay in Berlin using the Secure Information Exchange Network Application (**SIENA**) platform of Europol. In this message Van der Linde was (incorrectly) linked to terrorism. Europol was copied in for this message, as will be set out in more detail below.

21. At first, Van der Linde was not aware of any correspondence between the Dutch Police, the German police and Europol about him. In documents he received from the Municipality of Amsterdam after a data access request he discovered that the Dutch Police informed the BKA. Subsequently, Van der Linde filed a data access request with the Dutch Police on 3 September 2019, based on the Dutch Police Data Act (the Dutch implementation of the Law Enforcement Directive), seeking *inter alia* access to information about the way(s) his personal data was shared by the Dutch police with foreign authorities (**Annex A.10**).[15] In response to this request, the Police confirmed on 17 October 2019 that there were relevant files within the scope of this request

---

10 Decision Ministry of Justice and Safety, re. rectification NCTV, 7 September 2023, p. 2 (**Annex A.6**). In general, the Minister concluded that the NCTV had no legal basis for how it collected, processed and stored certain personal data in the period that Van der Linde's data was processed by the NCTV; *Kamerstukken II* ('Parliamentary documents') 2020-21, 30821, no. 131, pp. 6-10, URL: https://zoek.officielebekendmakingen.nl/kst-30821-131.pdf.

11 Judgment District Court of Amsterdam 3 November 2023, AMS 22/1390, pars. 15 and 16 (**Annex A.7**).

12 Letter Minister of Justice and Safety to Van der Linde, 30 June 2025, p. 2 (**Annex A.8**).

13 Letter Minister of Justice and Safety to Van der Linde, 30 June 2025, p. 3 (**Annex A.8**).

14 Decision Dutch Data Protection Authority, 12 March 2025, p. 1 (**Annex A.9**).

15 Letter Van der Linde to Police re. data access request, 3 September 2019 (**Annex A.10**).

and that these files were shared with the German Police and Europol (**Annex A.11**).[16] However, Van der Linde was only granted partial access to his file, and only by way of a personal visit to the station of the Regional Police Unit Amsterdam for viewing these documents. This visit took place on 23 October 2019. Van der Linde appealed the decision to grant partial access by the Police, as will be discussed further below.

22. Here, for the first time Van der Linde got an indication that his personal data was shared with Europol, and that he had been the subject of a SIENA message which was labelled "Crime area Terrorism". In practical terms: the Dutch Police effectively informed foreign authorities he should be perceived as a terrorist threat.

23. One of the documents Van der Linde was given access to (but was prohibited from copying) was SIENA message 1346846-1-1. This message, dated 29 May 2018, from the Netherlands Police Amsterdam Counter-Terrorism Unit (**CTER-unit**) to the Bundeskriminalamt CT in Germany, was sent to Europol in copy (CC). It should be noted that Van der Linde did not receive a copy of this message but was only allowed to look at it. The content of this message was described by the EDPS in its decision of 8 September 2022 and later on by the Dutch Police in its decision of 21 October 2022 (as discussed below)(**Annex A.12**).[17] On this basis, the content of this message can be described as follows.

24. In the message the Police writes that Van der Linde is a Dutch person of interest and that he is receiving medical treatment in Berlin (including the name and address of his therapist). The Police states that the reason why the BKA and Europol are informed is that he is a known leftwing activist who is included in the deradicalisation approach of the Municipality of Amsterdam, which as described above, was considered to be unlawful in his case. Because the Municipality is going to stop the social benefits Van der Linde receives to pay for his medical treatment in Berlin, the Police writes that, there is "a little concern" that he could undertake "(violent) action" against the government. The Police also writes that Van der Linde has no history of violence and that the Police does not have any signals that indicate a willingness to use violence on his part. Nonetheless, the Police wanted to give the BKA and Europol warning, but it does not require any action on their part. Nevertheless, the message in this context is highly suggestive, especially as this SIENA message contained the label "Crime Area: Terrorism" and was sent by the Dutch Counter Terrorism Unit to the Europol Counter Terrorism unit.

25. Along with this description by the Dutch Police of Van der Linde, effectively accusing him of being a terrorist or at least a dangerous extremist, the SIENA message included a personal file on Van der Linde from the Police as an attachment. The personal file contained information until 10 October 2017 on his involvement in various social media platforms, protests and initiatives against racism and discrimination. In addition, it contains information on (criminal) complaints he had filed regarding multiple death threats he received from right-wing extremists. Of importance is that

---

[16] Decision Police (annulled), 17 October 2019 (**Annex A.11**).

[17] Decision EDPS, 8 September 2022, par. 2.1 (**Annex A.2**); Decision Police (new), 21 October 2022, pp. 2-3, 5 (**Annex A.12**).

the message did not list any other crime areas under the header "Other crime area (out-of-mandate)".

26. In a separate case, of 8 April 2021, the District Court of Amsterdam ordered the Police to erase all references to "extremism" or similar terms in relation to Van der Linde from its systems (**Annex A.13**).[18] The Court ruled on this order after Van der Linde requested the Police to rectify the use of "extremism", "CTER" (which stands for Contra Terrorism, Extremism and Radicalisation), and "CTER04" (which stands for leftwing extremism) in relation to him and the Police refused to do so. As the Police failed to provide a justification for these qualifications to describe Van der Linde it failed to motivate its decision leading the Court to conclude that the decision to not rectify these qualifications was unsubstantiated.[19]

27. After this, Van der Linde also got a positive interim judgement in his appeal case against the decision by the Police to only grant him partial access to his case file containing the SIENA message. On 13 April 2022, the District Court of Amsterdam found the 2019 decision by the Police to be insufficiently substantiated and ordered the Police to take a new decision (**Annex A.14**).[20] This new decision was taken by the Police on 21 October 2022, providing Van der Linde with new information and granting him access to an additional part of his file which he had not previously been aware of.[21] From this, it *inter alia* became clear that in the period 2019-2021 the Police had sent various other messages about Van der Linde through the SIENA system.

28. In the new decision, the Police stated that after the Municipality removed Van der Linde from its deradicalization policy in March 2019, the Police sent a cancellation request to the BKA related to the SIENA message about Van der Linde from 29 May 2018 (the request was sent on 15 April 2019, SIENA message no. 1346846-1-2). However, no such request was sent to Europol. Only after Van der Linde sent an access request to Europol in 2020 did the Police requested Europol through two SIENA messages to delete the personal data it had shared with Europol about Van der Linde in 2018 (messages from 27 May 2020, 1346846-3-1 and 1346846-4-1). Despite this obvious error, the Police later suggested it made this request to Europol "out of diligence" ("*uit zorgvuldigheid*").[22] In addition, the Police notes it sent a SIENA message on 23 July 2021 to the BKA and Europol in which it states, pursuant to the Court decision of 2021 against the Police, that it has no interest in Van der Linde in relation to any form of extremism and that the Police has no information that Van der Linde poses a threat.[23] All these SIENA messages listed as crime area "Terrorism".

29. While the new decision contained more information than the first one, Van der Linde's request was still partially denied. Therefore, he requested the Court to proceed with the procedure on 20 November 2022 and submitted additional

---

18 Judgment District Court of Amsterdam 8 April 2021, AMS 19/2518, par. 10 (**Annex A.13**).

19 Judgment District Court of Amsterdam 8 April 2021, AMS 19/2518, par. 9 (**Annex A.13**).

20 Interim judgement District Court of Amsterdam 13 April 2022, AMS 19/6327 (**Annex A.14**). No final ruling has been issued in this case as of the moment of submitting the Application.

21 Decision Police (new), 21 October 2022 (**Annex A.12**).

22 Decision Police (new), 21 October 2022, p. 3 (**Annex A.12**).

23 Decision Police (new), 21 October 2022, pp. 2-3, 5 (**Annex A.12**).

arguments to obtain further access to information on the way his personal data was shared with the German police and other international agencies. Subsequently, the Court informed the parties on its intended judgment on 16 April 2024 (**Annex A.15**).[24]

30. In this letter, the Court harshly criticized the Police, finding "(very) significant differences" between the documents the Police initially shared with Van der Linde and the documents that were shared after the (first) appeal.[25] The Court noted, based on information provided by Van der Linde and its own knowledge, that this is "not an incident" but rather a structural issue.[26] The Court accepted Van der Linde's (substantiated) claim that there are still more relevant documents to be shared, which had not previously been shared and noted that there are structural deficiencies in the way the Police processes personal data. Such deficiencies were in violation of the Dutch Police Data Act. Previous independent research confirmed these conclusions.[27]

31. In an unprecedented step in the Dutch legal system, the Court therefore appointed an independent forensic IT expert. [28] This expert must assess whether the Police has conducted its search adequately and explain the big differences between the amount of documents found initially and on appeal and whether this is caused by failings of the Police.[29] In that context, the Court ordered the Police to grant the expert full access to the Police data systems and files where police data are kept. This investigation is ongoing.

32. A third case of relevance, besides those discussed above regarding Van der Linde's data access request concerning the SIENA messages and the rectification request in relation to extremism and CTER labels, followed from Van der Linde's rectification request of 15 November 2022 to the Police to correct the associations with terrorism that the Police made in its SIENA messages (**Annex A.16**).[30] The Police denied this request, *inter alia* arguing it had no other choice when sending the SIENA message than to select "Terrorism" in the field "Crime area"(**Annex A.17**).[31] Following the denial of this request, Van der Linde filed an appeal with the Court and also a complaint with the Police. This latter complaint led the Police to request Europol to change its form to allow for more options (**Annex A.18**).[32]

33. In the appeal case, the Court ruled on 12 March 2025 that the Police's decision needed to be annulled and ordered it to take a new decision (**Annex A.19**).[33] The Court ruled that the Police is aware that a lot went wrong in the case of Van der Linde. It stressed that the new decision should be taken with the utmost care and that the Police must limit his damage as much as possible.[34] In a message of 26 March 2025,

---

24 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, p. 3 (**Annex A.15**).
25 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, p. 4 (**Annex A.15**).
26 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, p. 4 (**Annex A.15**).
27 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, p. 4 (**Annex A.15**).
28 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, pp. 1, 5 (**Annex A.15**).
29 Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327 (**Annex A.15**).
30 Letter Van der Linde to Police re. rectification request, 15 November 2022 (**Annex A.16**).
31 Decision Police (annulled) re. rectification SIENA messages, 31 January 2023, p. 3 (**Annex A.17**).
32 Decision Police re. complaint, 11 April 2023 (**Annex A.18**).
33 Judgment District Court of Amsterdam 12 March 2025, AMS 23/990 (**Annex A.19**).
34 Judgment District Court of Amsterdam 12 March 2025, AMS 23/990 , par. 7 (**Annex A.19**).

in which the Police announced its intended appeal against this court order, the Police stated that it emphasized in all of its SIENA messages – including the 29 May 2018 message – that Van der Linde should not be considered radical or violent (**Annex A.20**).[35] On 29 September 2025 the Police finally took a new decision after it was ordered (again) by the Court to do so within two weeks on 17 September 2025 and was imposed a fine for each day the Police did not comply.[36]

34. In the new decision the Police indicated that it reached out twice to both the German police and Europol with the request to rectify the label "Crime area Terrorism" in all of Van der Linde's personal data they might have, because the label had no relation to the data subject and that he was not associated with terrorism (**Annex A.21**).[37] The Police also acknowledged that there existed three other SIENA messages about Van der Linde: two of which were sent by the German Police to the Dutch Police and one was the Dutch Police's response. Interestingly, the Police notes that only the Police's response was labelled with crime area terrorism.[38]

35. As such, Van der Linde's cases in the Netherlands have all had a similar dynamic: (1) his personal data is covertly processed in the context of extremism/terrorism by a public authority and shared with other authorities; (2) Van der Linde is forced to file data access requests to uncover the facts about his case, which are never immediately fully granted; and (3) based on the facts of the matter a Court and/or the authorities themselves find that the actions of the authorities were unlawful and steps must be taken to correct the consequences of their unlawful actions.

36. Unfortunately, as Van der Linde will show, the actions and omissions of Europol in his case share the same dynamic.

III.3 Background Europol and data subject access request to Europol

III.3.1 Background Europol

37. Europol is the law enforcement agency of the European Union. Europol's mission is to support Member States in preventing and combating all forms of serious international and organised crime, cybercrime, and terrorism. To this end it facilitates the exchange of information and intelligence, provides analytical support, and offers specialized training and expertise to Member State law enforcement agencies. To ensure effective cooperation between Europol and Member States a national unit functions as the liaison link between them.

38. Europol makes use of the "Europol Analysis System" (**EAS**), which it describes as an information processing system.[39] Within EAS, so-called "Analysis Projects" (**AP**) exist which focus on certain crime areas. The aim of these Analysis Projects is to help tackle organised crime and terrorism by *inter alia* analysing data in the projects and sharing information between project partners. One Analysis Project is called "Dolphin" (**AP**

---

35 E-mail Police to Van der Linde re. intended appeal, 26 March 2025, p. 1 (**Annex A.20**).

36 Judgment District Court of Amsterdam 17 September 2025, AMS 25/2901 (not included as annex).

37 Decision Police (new), 29 September 2025, p. 4 (**Annex A.21**).

38 Decision Police (new), 29 September 2025, p. 5 (**Annex A.21**).

39 All descriptions of EAS and Analysis Projects are taken from Europol's own information: Europol, 'Europol Analysis Projects', last updated: 14 August 2025, last accessed: 6 October 2025, URL: https://www.europol.europa.eu/how-we-work/europol-analysis-projects.

Dolphin). AP Dolphin is aimed at "Combatting Terrorism and Extremism" and according to Europol "focuses on gathering information on both intelligence and law enforcement levels of non-Islamic terrorism activities".[40]

39. The Secure Information Exchange Network Application (**SIENA**), maintained by Europol, is a messaging system used by European police forces to send encrypted messages to each other and to Europol.[41] As of 13 August 2025, more than 3.500 national competent authorities from 53 countries and 16 international organisations are connected to the SIENA system.[42] They can exchange messages about individuals, and they have access to information stored by Europol. In addition, in the beginning of 2022 the specific SIENA framework handling restricted content on counter-terrorism had forty-nine counter-terrorism authorities connected to the dedicated SIENA counter-terrorism environment. [43]

40. There is little specific public information about the operation of SIENA. This is caused (at least in part) by the fact that Europol does not allow individual Member States to answer questions about the SIENA system. As the owner and administrator of the SIENA system, Europol is of the opinion that questions about SIENA should be directed to, and answered by, Europol only (**Annex A.22**).[44] The Police was informed of this by Europol after the Police had already informed Van der Linde that if a Member State wants to send a message via the SIENA system, it must select a "Crime Area" that the message relates to from an exhaustive list of options.[45] In response to questions, Europol confirmed "[t]here is a procedure in place to reject SIENA messages not falling under the mandate of Europol" (**Annex A.23**).[46]

III.3.2 Data subject access request to Europol

41. As set out in the above, on 29 May 2018 the Police sent a message to the BKA using SIENA about Van der Linde, copying in (CC) Europol, and using the label "Crime area Terrorism". By processing this SIENA message, Van der Linde automatically got an "active" status from Europol for half a year. Van der Linde became aware of the existence of a message sent to Europol on 17 October 2019 and got access to its content on 23 October 2019. Upon becoming aware of this message, Van der Linde filed a data subject access request to Europol on 11 February 2020 (**Annex A.24**).[47] On 11 June 2020, Europol replied to Van der Linde, stating "there are no data concerning you at Europol to which you are entitled to have access in accordance with Article 36 of the Europol Regulation" (**Annex A.25**).[48]

---

[40] Europol, 'Europol Analysis Projects', last updated: 14 August 2025, last accessed: 6 October 2025.

[41] Europol, 'Secure Information Exchange Network Application (SIENA)', last updated: 13 August 2025, last accessed: 6 October 2025, URL: https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena.

[42] Europol, 'Secure Information Exchange Network Application (SIENA)', last updated: 13 August 2025, last accessed: 6 October 2025.

[43] Europol, 'Secure Information Exchange Network Application (SIENA)', last updated: 13 August 2025, last accessed: 6 October 2025.

[44] E-mail Police to Van der Linde re. the SIENA system, 9 November 2023 (**Annex A.22**).

[45] Decision Police (annulled) re. rectification SIENA messages, 31 January 2023, p. 3 (**Annex A.17**).

[46] E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025, p. 2 (**Annex A.23**).

[47] Letter Van der Linde to Europol re. data access request, 11 February 2020 (**Annex A.24**).

[48] Decision Europol refusing data access, 11 June 2020 (**Annex A.25**).

42. Van der Linde then filed a complaint against Europol with the European Data Protection Supervisor (**EDPS**) on 6 October 2020 on the handling of his data access request by Europol (**Annex A.26**).[49] It took the EDPS more than two years to investigate the complaint and it published the results of its investigation on 8 September 2022.[50] Below the findings of the EDPS will be reproduced in some detail, as it provides a comprehensive understanding of the actions of Europol, both in processing Van der Linde's personal data and the handling of his data access request.

III.4 Decision EDPS on complaint Van der Linde against Europol

43. The EDPS investigation led to a striking condemnation of Europol. The facts underlying the EDPS decision were as follows (all references in text are to the EDPS decision unless stated otherwise).[51] These events were unknown to Van der Linde at the time they occurred.

III.4.1 Handling of data subject access request by Europol

44. On the same day Europol received the data subject access request from Van der Linde via the Dutch Police (10 March 2020), which it also received directly from him on 11 February 2020, Europol searched its systems for data on Van der Linde. This revealed a "full hit" on Van der Linde in AP Dolphin, with a person "implication of suspect" (par. 2.5). The EDPS noted that AP Dolphin gathers intelligence and information related to "terrorist groups" and "other violent extremist groups active in the EU" (footnote 12).

45. On 11 March 2020, the data protection unit at Europol, the so-called Data Protection Function (**DPF**), reached out to the Liaison Bureau Netherlands and asked whether "the Netherlands competent authority would agree to the release of information to" Van der Linde (par. 2.6). The Bureau did not reply, after which the DPF set up a videocall on 25 May 2020 with operational staff from AP Dolphin. AP Dolphin "informed the DPF that they would follow up with Liaison Bureau Netherlands regarding their position on disclosure of the personal data" (par. 2.6). In the call, AP Dolphin provided its opinion that the information should not be released (par. 2.6).

46. Also on 25 May 2020, the Data Protection Officer (**DPO**) of the Dutch Police contacted Europol to ask why Europol was still processing Van der Linde's personal data after the SIENA message had been cancelled (par. 2.7). It was then determined by the Police that "Europol was still in possession of the data due to an error" (par. 2.19). On 27 May 2020, the Netherlands sent a request to Europol through SIENA to delete all data of Van der Linde mentioned in the SIENA message from 29 May 2018 (1346846-1-1) and the cancellation SIENA message (1346846-3-1) (par. 2.7). This contained his personal data associating him with terrorism and revealing information about his health care situation and political views. The Netherlands noted that "the pending procedure to consult the Dutch Police on disclosure could be solved if Europol would delete the information from its Analysis System" and the Dutch CTER-unit asked Europol to "let them know whether the deletion could be a solution to the

---

[49] Complaint Van der Linde to EDPS against Europol 6 October 2020 (**Annex A.26**).
[50] Decision EDPS, 8 September 2022 (**Annex A.2**).
[51] Decision EDPS, 8 September 2022 (**Annex A.2**).

problem" (par. 2.7). On 28 May 2020 AP Dolphin informed the DPF "that the data in the cancelled SIENA message had been deleted" (par. 2.7).

47. Considering the fact that Van der Linde has never been a suspect of terrorism, it is striking that his data is associated by Europol with projects that all relate to terrorism. Especially since the Dutch Police is of the opinion that it was clear enough from the content of the SIENA messages that the Dutch Police did not associate Van der Linde with terrorism,[52] and that it emphasised, according to the Police, in every SIENA message that it did not consider Van der Linde to be radical or violent.[53] This was later also conveyed to Europol via the SIENA message from 23 July 2021 stating that the Dutch Police has no interest in Van der Linde in relation to any form of extremism whatsoever.[54]

48. On 3 June 2020, the DPF checked EAS to verify the deletion of Van der Linde's personal data. However, this check led to the discovery that more personal data of Van der Linde was present in the Europol systems. Parts of the EDPS decision on this point have been blacked out but from the decision Van der Linde can gather the following (par. 2.4).

49. The Netherlands had provided Europol with a mobile phone in an ongoing investigation on 7 February 2020, asking for support to extract data from the device and to store it. The information subsequently extracted from the device and stored by Europol included personal data from Van der Linde's Twitter account, which was stored in a "data file" in EAS (par. 2.4). In the EDPS decision, this is referred to as "a second item of personal data"(par. 2.8). It is unclear to Van der Linde what exactly this entails: it may be a complete extract of all posts on his Twitter account, and/or possibly other personal data.

50. It is unclear where in the EAS Van der Linde's Twitter account data was stored exactly, as Europol itself could not find "the origin and relevance of the information on the complainant's Twitter account" during the EDPS investigation (par. 2.8). The DPF subsequently contacted AP Dolphin, AP Hydra (focused on "terrorism-related crimes […] perpetrated by individuals, groups, networks or organisations who evoke Islam to justify their actions"[55]), AP TFTP (focused on "tracking terrorist money flows"[56]) and EU IRU ("detects and investigates malicious content on the internet and in social media" focusing on "[t]errorists' use of the internet and social media"[57]) about this data. Specifically, the DPF requested whether "(i) the data on the Twitter account was relevant from an operational point of view and needed to be stored in the EAS; and (ii) whether information on the storage of the Twitter account could be released to" Van der Linde (par. 2.8).

---

52 Decision Police (annulled) re. rectification SIENA messages, 31 January 2023, pp. 3-4 (**Annex A.17**).

53 E-mail Police to Van der Linde re. intended appeal, 26 March 2025, p. 1 (**Annex A.20**).

54 Decision Police (new), 21 October 2022 (**Annex A.12**).

55 Europol, 'Europol Analysis Projects', last updated: 14 August 2025, last accessed: 6 October 2025.

56 Europol, 'Europol Analysis Projects', last updated: 14 August 2025, last accessed: 6 October 2025.

57 Europol, 'EU Internet Referral Unit – EU IRU', last accessed: 6 October 2025, URL: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru.

51. The European Counter Terrorism Centre (**ECTC**) at Europol, where the EU IRU is based, eventually decided to delete this information from the EAS (but it turned out it was not actually erased, but only deleted, as will be discussed below) (par. 2.9). On 5 June 2020, the ECTC replied to Europol's request that the Twitter account "was not relevant from an operational point of view and could be deleted from EAS" (par. 2.9). The ECTC disagreed with providing Van der Linde any information, because it claimed (i) the data would be deleted and (ii) not giving access would guarantee that no national ongoing investigations would be jeopardized.

52. In response, the DPF requested the data to be deleted as soon as possible. The ECTC communicated to the DPF on the same day "that it had deleted the data concerned from the EAS" (par. 2.9).

53. Finally, on 5 June 2020 the DPF sent an internal briefing note "informing the Executive Director of a full hit (positive match) in its systems following a data subject access request, the procedures followed in accordance with Article 36 of the Europol Regulation to handle the request, and the assessment and proposed response to the data subject" (par. 2.10). The DPF recommended to refuse access to Van der Linde based on art. 36(6)(a) ER (i.e. refusal necessary to enable Europol to fulfil its tasks properly) (par. 2.10). On 11 June 2020, Europol sent its refusal to Van der Linde: "There are no data concerning you at Europol to which you are entitled to have access in accordance with Article 36 of the Europol Regulation" (par. 2.11). No motivation or reasons for this decision were provided.

54. Van der Linde was not informed that there were two hits for his personal data in the Europol systems. He was also not informed that Europol has discussed his request with the Dutch authorities and that their "solution" to the "problem", the problem being Van der Linde's data access request, is to simply delete his data. He only knew, as a result of his data subject access request to the Dutch Police, that Europol had at some point processed his personal data, in any case by receiving the 29 May 2018 SIENA message. And he got a brief refusal of his request on 11 June 2020.

III.4.2 EDPS investigation

55. On 20 October 2020, the EDPS requested comments from Europol on Van der Linde's complaint, after which Europol confirmed to the EDPS on 11 November 2020 that it had been processing Van der Linde's personal data at the time it received his data subject access request and that it had subsequently deleted that data. Europol furthermore "identified the Netherlands as the contributor of the personal data" and "provided reasons for its decision to refuse access" (par. 1.3-1.4). The EDPS requested further information on the timing of the decision to delete the data of Van der Linde and screenshots to prove that his data was no longer being processed in Europol's systems (par. 1.5). In response to these requests, Europol sent two print screens from its systems Palantir and iBase "as evidence that no personal data on" Van der Linde was processed at the current time and clarified that the decision to delete the data was taken after Van der Linde's access request and after consultation with the Netherlands (par. 1.6).

56. From the EDPS' description of its investigation, it becomes apparent the EDPS struggled to get information from Europol on (at least) two issues. Firstly, the EDPS

had difficulties in getting Europol to provide access to the data on Van der Linde that Europol processed at the time of receipt of his data subject access requests. The EDPS sent multiple requests to Europol to provide a copy of this data via a secure channel, but Europol refused to transmit this data. Europol instead invited the EDPS to come to Europol headquarters to verify the data (par. 1.8-1.14). Eventually, on 22 June 2021 two Europol staff members visited the EDPS "in order to provide access to the requested documents on a secure Europol laptop". During this visit "the EDPS viewed the operational personal data concerning the complainant (SIENA messages and a personal file on the complainant) and correspondence between the DPF, Europol operational units, Liaison Bureau Netherlands (LB NL) and the Dutch Police". This "email correspondence was consulted on screen during a secure videoconference call with Europol's DPF during the visit" (par. 1.15).

57. During this visit, Europol explained to the EDPS how it was possible to still retrieve this data despite having deleted it previously. With regards to Van der Linde's Twitter account, Europol explained that this could be found "via a targeted search in the EAS because this personal data was still stored in the raw document extracted from the mobile phone" (par. 2.20). Regarding the deleted SIENA messages, "Europol explained that the set of data related to the case will only be deleted when a new data retention functionality ('the EAS SIENA data retention synchronisation') is implemented" (par. 2.20). Until that moment the data was thus still accessible in Europol's data retention system.

58. The second issue that came up during the EDPS investigation was getting information on the reasons for refusing Van der Linde access to his data and the internal assessment that documented the exemption under art. 36 ER on which the refusal was based, but which was not shared with Van der Linde. The EDPS had to send Europol multiple requests for this information as well as multiple clarification requests (par. 1.7-1.14).

59. During its investigation, the EDPS contacted the Dutch Data Protection Authority (Dutch Supervisory Authority, **Dutch SA**). The EDPS requested information (i) on the lawfulness of the transmission of the data to Europol and (ii) on whether Van der Linde could be granted access to his information or that the exemptions in art. 36 ER applied (par. 1.7). On 16 April 2021, the Dutch SA informed the EDPS that it had "encountered difficulties in locating the required information", for example that it could find no record "of Europol's consultation of the Dutch police under Art. 36(5) of the Europol Regulation" nor "of the transmission of personal data on the complainant to Europol by the Dutch competent authorities" (par. 2.21). As such, the Dutch SA informed the EDPS that it "could not provide an opinion regarding the lawfulness of transmission of the personal data from the Netherlands to Europol" (par. 2.21). With regards to the second question posed by the EDPS, the Dutch SA "relayed the position of the Dutch police that "the data shared with Germany on the data subject is of such nature (counter-terrorism information) that it cannot be disclosed to him"" (par. 2.21).

60. After receiving this reply by the Dutch SA, the EDPS asked Europol additional questions "including [on] discrepancies between information provided by the Dutch SA and information provided by Europol" (par. 1.11). This led to Europol finally

sharing a copy of its internal assessment, which was followed by additional requests for clarification by the EDPS (par. 1.12-1.13). The EDPS also forwarded the internal assessment document to the Dutch SA and requested it "to complete its checks on the personal data processed" on Van der Linde (par. 1.14). This resulted in a letter by the Dutch SA to the EDPS on 14 September 2021 with a revised opinion, deviating from its conclusion from 16 April 2021 (par. 1.16).

61. In this revised opinion, the Dutch SA wrote that "follow-up consultations with the Privacy Officer of the Netherlands Police's Central Unit had located the two items of personal data concerning the complainant and transmitted by the Netherlands competent authority to Europol in 2018 and 2020" (par. 2.22). According to the Dutch SA, it "can agree with the Netherlands police's assessment that both transmissions were lawful" (par. 2.25). Furthermore, as Van der Linde already had access in 2019 to a copy of the data in the SIENA message, the Dutch SA explained that "the NL police does not see the need for keeping this information from him or calling in restrictions for that matter" (par. 2.23). With regards to the data on his Twitter account, the Dutch SA informed the EDPS that the position of the Dutch Police is that "no restrictions in releasing the information to the complainant are necessary, as in principle it could happen to anyone that his personal data from a social media account turn out to be stored on a device of person [sic] who has become a target of interest to law enforcement" (par. 2.24).

62. The EDPS forwarded the Dutch SA's revised opinion to Europol and requested Europol to review, based on that new opinion, its original decision to refuse Van der Linde access to his data (par. 1.17). The EDPS granted Europol two extensions of the deadline for this reassessment, after which the EDPS sent three reminders before receiving Europol's reassessment (par. 1.17-1.19). On 11 February 2022 Europol shared the results of its reassessment. Europol decided to uphold "the initial decision-making that led to its decision to refuse access", but, in light of the second opinion of the Dutch SA, "comes to the conclusion that there are no aspects for Europol to divert from the opinion of the NL data protection authority, i.e. that there are no reasons to refuse access to the information with respect to the data subject" (par. 2.16).

63. Europol also proposed a reply to Van der Linde, namely that Europol has "reassessed its position as regards the access request", to confirm to Van der Linde that Europol "had been processing data on him originating from the Dutch law enforcement authorities at the time of his request" and inform Van der Linde "that these personal data had been deleted on 5 June 2020". Europol proposed that for any further information, Van der Linde should be advised to address the Dutch SA (par. 2.18).

64. Europol then informed the EDPS that as it had deleted Van der Linde's data on 5 June 2020, it considered it "appropriate that the data subject is referred to the competent authorities in NL". Moreover, Europol stated "that it had established that on 7 February 2022, "there is no information on the data subject processed in Europol's operational systems at this moment in time, in line with the procedure agreed with the EDPS" (par. 2.17).

65. The EDPS finally presented its findings on 8 September 2022 to Van der Linde. The EDPS "strongly underlines that no such procedure was discussed or agreed with

Europol during the complaint investigation with respect to the deletion of the complainant's personal data" (par. 3.48) and "further underlines that should Europol have erased (permanently deleted) the personal data concerning the complainant, this would constitute a failure to cooperate with the EDPS and a serious infringement of the Europol Regulation" (par. 3.50). If, alternatively, Europol simply meant the personal data of Van der Linde is archived, "it should have been considered as existing for the purpose of the complainant's access request" (par. 3.49).

66. The legal conclusions from the decision of the EDPS will be further elaborated on below. In short, the EDPS found that Europol insufficiently motivated its decision, wrongly referred part of Van der Linde's request to the Dutch Police, failed to provide all information, potentially wrongfully deleted information, should retrieve the deleted information and has breached the Europol Regulation and the EU Charter (pars. 3.19-3.21, 3.23-3.29, 3.31-3.32, 3.58-3.60).

67. Moreover, the EDPS concluded that it has "grounds to understand that even data which is deleted from Europol's operational systems is nevertheless searchable and retrievable by Europol, from its databases, back-up systems or archives" (par. 3.51). During its investigation, the EDPS has found indications "that Europol does not implement a consistent policy of hard deletion, i.e. erasure of personal data", but that it, once it "assesses that data can no longer be stored under Article 31 of the Europol Regulation", "soft deletes" data "meaning that it is marked so that users cannot access them, but nevertheless retained in those databases" (par. 3.52). Later, it was confirmed by Europol that it has stored the supposedly deleted data of Van der Linde in a separate, access-restricted location, isolated from Europol's operational systems for the handling of the complaint procedures (**Annex A.27**).[58]

68. Both Van der Linde and Europol have asked the EDPS for a revision of this decision (**Annex A.28**).[59] Europol's reasons for asking revision relate to the access Van der Linde should get according to the EDPS decision. According to Europol, the EDPS concluded that Van der Linde has already had full access to the SIENA message in 2019 and his access should thus not be restricted now. This is incorrect according to Europol, as Van der Linde has not seen the entire SIENA message and its attachment, which was partly redacted.

69. On 30 January 2023 the EDPS concluded that Van der Linde's request for revision "has identified new elements that require analysis, in particular with regard to the alleged lack of a documented assessment of the lawfulness of processing of your personal data by Europol" and that therefore, the EDPS will re-examine its decision (**Annex A.29**).[60] With regards to the information underlying Europol's revision request, the EDPS noted that Europol has provided documents it had not provided before the EDPS had issued its decision. This information related in particular to "the extent of

---

[58] Letter Europol to Van der Linde, 3 February 2025 (**Annex A.27**); and also Decision Police (new), 29 September 2025, p. 4 (**Annex A.21**).

[59] E-mail EDPS to Van der Linde, 21 October 2022 (**Annex A.28**). In November 2022 Van der Linde was compelled to file for annulment of the EDPS decision with the CJEU but this was later discontinued as the EDPS decided to review its decision and Van der Linde was reassured of the scope and depth of the reopened investigation.

[60] Decision review EDPS, 30 January 2023, pp. 1-2 (**Annex A.29**).

prior disclosure by the Dutch authorities to the complainant of the information contained in SIENA message 1346846-1-1 and the position of the Dutch competent authorities vis-à-vis the prospect of full disclosure".[61] The EDPS noted that these new documents "contradict the final position of Europol on the matter of access to be granted to the complainant" despite Europol having access to this information.[62] The EDPS found that Europol had "ample time and opportunity to transmit those elements to the EDPS during the course of its investigation" and as such "would not be sufficient to classify a request for a review as admissible".[63] The EDPS decided to also re-examine its decision in light of the new elements introduced by Europol "due to the legitimate interests of public order and public security at stake in this matter", "without this decision in any way constituting a precedent".[64] The EDPS however decided to suspend the review of its earlier decision in light of the pending case before the Court of Amsterdam between Van der Linde and the Police.

70. After all the above, it was still not fully clear to Van der Linde how Europol had processed his personal data and he sent a number of questions to Europol (DPF) (**Annex A.30**).[65] In response, the DPF stated that Europol has access to the content of SIENA mailboxes of all Europol entities and "handles requests of data subjects for access, rectification and erasure in regard to those mailboxes".[66] Furthermore, Europol "is responsible for all data processing operations carried out by it, with the exception of the bilateral exchange of data using Europol's infrastructure between Member States, Union bodies, third countries and international organisations to which Europol has no access".[67] After further questions, the DPF explained how Europol views its legal responsibilities for SIENA messages it receives in copy:[68]

> "The provision of a message to Europol in CC does not switch the legal responsibility from the sender of the message to Europol. The right of access concerning such a message can be exercised both to the sender and to Europol (when Europol is in CC)."

III.5 Cases before EDPS and Court of Amsterdam

71. The outcome of legal proceedings in the Netherlands and proceedings before the EDPS are separate from the present case but may result in additional facts that may be of relevance while the present case proceeds further. Van der Linde therefore briefly sets out the substance of these cases.

72. In administrative proceedings before the District Court of Amsterdam pursuant to a data subject access request, the Court appointed a forensic IT expert to go through police systems and see whether all information that falls under the three information

---

61 Decision review EDPS, 30 January 2023, p. 2 (**Annex A.29**).
62 Decision review EDPS, 30 January 2023, p. 2 (**Annex A.29**).
63 Decision review EDPS, 30 January 2023, p. 2 (**Annex A.29**).
64 Decision review EDPS, 30 January 2023, p. 2 (**Annex A.29**).
65 E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025 (**Annex A.23**). Also see Complaint Van der Linde against Europol, 3 February 2025 (**Annex A.30**).
66 E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025, p. 4 (**Annex A.23**).
67 E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025, p. 4 (**Annex A.23**).
68 E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025, p. 1 (**Annex A.23**).

requests of Van der Linde has been found.[69] Only one of those three information requests relates to the SIENA messages. The Court informed the parties by letter of 3 June 2025 that an independent forensic expert has started the investigation (**Annex A.31**).[70] Once the expert has concluded its work, the Court will issue a ruling on the decision making of the Police in the context of the data subject access request.

73. The EDPS has decided to suspend the process of revision of its 8 September 2022 decision, finding that the case before the Court of Amsterdam deals "partially with the same matter now under consideration by the EDPS".[71] It has informed Van der Linde that its investigation will continue in the meanwhile.

74. As such, these cases are linked to, but also clearly separate from the present Action for damages. The case before the **District Court of Amsterdam** is an administrative procedure that primarily focuses on Van der Linde's data subject access request to the Police about what data has been shared with the German and other international authorities. After a judgment is rendered in that case, the **EDPS** will come to a decision in the revision case described above, which is about the lack of documented assessment of the lawfulness of processing of Van der Linde's personal data by Europol. As such, these cases are clearly delineated and separate from the current case, in which Europol is held liable for the damage it caused to Van der Linde for the reasons stated herein. The facts, as presented in this chapter, are clear and more than sufficient to hold Europol liable for its unlawful conduct, as detailed in the following chapters.

IV. LEGAL FRAMEWORK

IV.1 Action for damages – non-contractual liability rules

75. This Action for damages is based on art. 268 TFEU read in conjunction with art. 340 TFEU. Van der Linde derives his right to compensation for the damage as a result of Europol's unlawful conduct from art. 340 TFEU and arts. 49(3) and 50(1) ER.

76. Art. 340 TFEU sets out the general rule on non-contractual liability for the Union. Art. 49(3) ER contains an independent but similar legal ground for non-contractual liability of Europol. Art. 50(1) ER provides a specific legal basis for non-contractual liability for unlawful personal data processing by Europol. The Court of Justice of the European Union (**CJEU**) held in the *Kočner/Europol* case that art. 49 ER is a more general rule that is without prejudice to the specific liability rule of art. 50 ER.[72]

77. In its case-law the CJEU has developed the conditions under which the EU incurs non-contractual liability that are in accordance with the general principles common to the laws of the Member States.[73] In *Kočner/Europol*, a case of particular relevance to the current proceedings as it also concerned an action for damage against Europol, the

---

[69] Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327, p. 4 (**Annex A.15**).

[70] Letter District Court of Amsterdam re. investigation forensic expert, 3 June 2025, p. 1 (**Annex A.31**).

[71] Decision review EDPS, 30 January 2023, p. 3 (**Annex A.29**).

[72] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 66. The CJEU considered the reference in art. 49(3) to art. 49 an obvious drafting error. The legislator meant to refer to art. 50 ER, which derogates from the general rule.

[73] See for instance judgement of 8 January 2025, *Bindl v European Commission*, T-354/22, EU:T:2025:4, par. 48.

CJEU detailed those conditions. The first being the existence of a sufficiently serious breach of a rule of law intended to confer rights on individuals, the second the fact of damage and the third the existence of a causal link between the breach of the obligation resting on the author of the act and the damage sustained by the injured parties.[74] These conditions are discussed in detail below.

IV.1.1 Condition of unlawful conduct

78. The existence of unlawful conduct is a first condition for non-contractual liability. Concerning the general rules on non-contractual liability, based on art. 340 TFEU and art. 49(3) ER, the CJEU clarified that this first condition (the unlawfulness of the conduct) consists of two parts, namely that it is necessary (i) that a breach of a rule of EU law intended to confer rights on individuals has occurred and (ii) that that breach is sufficiently serious.[75]

79. In relation to liability based on art. 50(1) ER it must be noted that from this provision it follows that the condition of unlawful conduct is understood as "an unlawful data processing operation". The CJEU held in this regard, in *Kočner/Europol,* that an individual need to establish only that unlawful data processing took place in the context of cooperation involving Europol and a Member State.[76]

80. The CJEU held that the limiting in this provision of what an applicant needs to establish to meet the first condition of liability follows from the Europol Regulation. It held that in order not to deprive art. 50(1) of its effectiveness applicants "cannot be required to establish to whom, out of Europol or the Member State concerned, that damage is attributable".[77] This relates to the question of joint and several liability.

81. Lastly, it is noted that an omission can also be unlawful. Omissions can give rise to liability on the part of the European Union as far as the institutions have failed to fulfil a legal obligation to act under an EU law provision, the CJEU has held.[78]

82. The two parts of the first condition of liability are discussed in more detail below.

IV.1.1.1 Breach of rule of law intended to confer rights on individuals

83. It is well established case-law, as the CJEU emphasized in *Kočner/Europol*, that "the rights of individuals arise not only where they are expressly granted by provisions of EU law, but also by reason of positive or negative obligations which those provisions impose in a clearly defined manner, whether on individuals, on the Member States

---

[74] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, pars. 73 and 117; and Judgment of 10 September 2019, *HTTS v Council*, C-123/18 P, EU:C:2019:694, par. 32; and Judgment of 16 December 2020, *Council v K. Chrysostomides & Co. and Others*, C-597/18 P, C-598/18 P, C- 603/18 P and C-604/18 P, EU:C:2020:1028, pars. 79-80 and the case-law cited.

[75] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 118, and referencing Judgment of 10 September 2019, *HTTS v Council*, C 123/18 P, EU:C:2019:694, par. 36.

[76] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 74.

[77] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 76, see also par. 80.

[78] Judgment of 29 January 1998, *Dubois et Fils v Council and Commission*, T-113/96, EU:T:1998:11, par. 56; Judgment of 6 December 2001, *Area Cova SA and Others v Council and Commission*, T-196/99, EU:T:2001:281, par. 84; Judgment of 26 February 2016, *Šumelj and Others v Commission*, T-546/13, EU:T:2016:107, pars. 39-42; Also see Judgment of 15 September 1994, *KYDEP v Council and Commission*, C-146/91, EU:C:1994:329, par. 58.

or on the EU institutions, bodies and agencies […]. That rule also applies to obligations imposed by EU law in the context of cooperation between an agency of the European Union, such as Europol, and the Member States."[79]

84. Provisions of EU law can thus implicitly confer rights on individuals that might be negatively affected by a breach of obligations of EU agencies. The CJEU held that the full effectiveness of those rules of EU law and the protection of the rights which they are intended to confer require that individuals have the possibility of obtaining redress.[80]

85. Thus, the first part of the first condition is met if Europol breaches a right of Van der Linde or its obligation that implicitly confers rights on Van der Linde.

IV.1.1.2 Sufficiently serious breach

86. The CJEU clarified the second part of the condition of unlawful conduct in the *Kočner/Europol* case as it held that the decisive criterion for finding that a breach is sufficiently serious is that there must have been a manifest and grave disregard for the limits of the discretion laid down by the rule infringed.[81] This means that as the discretion of an agency is more limited, the threshold for a breach to be sufficiently serious will be passed sooner.[82]

87. The assessment of whether a breach was sufficiently serious needs to take account of (i) the field, circumstances and context of the obligation that has been breached, (ii) the degree of clarity and precision of the violated rule, (iii) the measure of discretion left by that rule, (iv) the complexity of the situation to be regulated, and (v) difficulties in the application or interpretation of the legislation.[83] In *Bindl/European Commission* the General Court also listed as an element to take into account (vi) whether the error of law was inexcusable or intentional.[84]

88. The purpose of this requirement is to avoid that the risk of having to bear the losses claimed by the persons concerned obstructs the ability of the institution concerned

---

79 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 119, and referencing Judgment of 22 December 2022, *Ministre de la Transition écologique and Premier ministre (Liability of the State for air pollution)*, C-61/21, EU:C:2022:1015, par. 46. Also see for example Judgment of 8 January 2025, *Bindl v European Commission*, Case T-354/22, EU:T:2025:4, par. 50.

80 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 120, and referencing judgement of 22 December 2022, *Ministre de la Transition écologique and Premier ministre (Liability of the State for air pollution)*, C-61/21, EU:C:2022:1015, par. 47.

81 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 126; Also see judgement of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 52.

82 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 126, and referencing judgement of 4 July 2000, *Bergaderm and Goupil v Commission*, C-352/98 P, EU:C:2000:361, par. 43; Judgment of 4 April 2017, *Ombudsman v Staelen*, C-337/15 P, EU:C:2017:256, par. 31; Judgment of 10 July 2003, *Commission* v *Fresh Marine*, C-472/00 P, EU:C:2003:399, par. 26; And judgement of 30 January 1992, *Finsider and Others v Commission*, C-363/88 and C-364/88, EU:C:1992:44, par. 22.

83 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, pars. 127-128, and referencing judgement of 4 April 2017, *Ombudsman v Staelen*, C-337/15 P, EU:C:2017:256, par. 40; Judgment of 30 May 2017, *Safa Nicu Sepahan v Council*, C-45/15 P, EU:C:2017:402, par. 30; And judgement of 19 April 2007, *Holcim (Deutschland) v Commission*, C-282/05 P, EU:C:2007:226, par. 50.

84 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 53.

to exercise to the full its powers in the general interest without, however, thereby leaving individuals to bear the consequences of flagrant and inexcusable conduct.[85]

89. Thus, the second part of the first condition is met if Europol has manifestly and gravely disregarded the limits of its discretion laid down by the rule infringed, it being a right of individuals or an obligation of Europol that implicitly confers rights on individuals.

IV.1.2 Condition of damage

90. The CJEU has long standing case-law from which it follows that the condition of damage requires genuinely suffered actual and certain damage.[86] This was recently confirmed in *Bindl/European Commission*, where the General Court further noted that purely hypothetical and indeterminate damage does not give rise to compensation.[87]

91. Damage can consist of material and non-material damage. Non-material damage may consist of injury to someone's mental health (psychological damage) and injury to someone's personal integrity, including because of realistic and profound anxiety.[88] In addition, it can also consist of impairment of the someone's image, honour, and reputation.

92. The General Court did rule that for "actual non-material damage allegedly suffered, it should be recalled that, while offering evidence is not necessarily held to be a condition for the recognition of non-material damage, it is for the applicant at least to establish that the conduct alleged against the institution concerned was capable of causing him such damage".[89]

93. The condition of damage is thus met if Van der Linde genuinely suffered actual and certain damage.

IV.1.3 Condition of causal link

94. The CJEU has established that the causal link, as third condition for liability, must be sufficiently direct. In *Bindl/European Commission* the General Court recently held that this concerns a sufficiently direct causal nexus between the conduct of the institution complained of and the damage so that the conduct complained of must be the determining cause of the damage.[90] Furthermore, in *Keserű Művek Fegyvergyár Kft./European Union*, the General Court considered more specifically

---

85 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 51.

86 Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 135, and referencing judgement of 30 May 2017, *Safa Nicu Sepahan v Council*, C 45/15 P, EU:C:2017:402, pars. 61 and 62. Also see judgement of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 54.

87 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 54.

88 Judgment of 8 November 2011, *Idromacchine and Others v Commission*, T-88/09, EU:T:2011:641, pars. 91-93.

89 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 81.

90 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 55.

that the damage must flow sufficiently directly from the unlawful conduct, which excludes damage which is only a remote consequence of that conduct.[91]

95. In particular, in cases where the alleged damage was caused by an omission, it must be certain that that damage was actually caused by the omission and could not have been caused by another act. [92]

96. This third and final condition of liability is thus met if the unlawful conduct (or omission) of Europol is in a sufficiently direct link with Van der Linde's damage and that it is the determining cause of the damage.

IV.2 Europol Regulation

97. The Europol Regulation went into effect on 13 June 2016. The unlawful conduct by Europol occurred in 2018, as Europol processed personal data of Van der Linde in May 2018, and in 2020, when he requested his information and Europol subsequently unlawfully rejected his request in June 2020. This makes that the Europol Regulation of 2016 is applicable. The Europol Regulation was amended by Regulation (EU) 2022/991 that went into effect on 28 June 2022. All references to the amended Europol Regulation are followed by "(2022)". Where reference is made to the Europol Regulation this refers to the version of 2016.

98. Based on art. 88 TFEU (former art. 30 TEU) the European Parliament and the Council of the EU have adopted the Europol Regulation. Art. 88 TFEU also establishes Europol's mission and tasks. In the Europol Regulation itself the European legislator further defined Europol's mission by including its objectives (art. 3 ER) and specifying its tasks (art. 4 ER).

99. Provisions of special relevance to this case are, besides those containing definitions (art. 2 ER), those that establish obligations on Europol and rights of individuals:

    Art. 17 Sources of information,
    Art. 18 Purposes of information processing activities,
    Art. 19 Determination of the purpose of, and restrictions on, the processing of information by Europol,
    Art. 28 General data protection principles,
    Art. 30 Processing of special categories of personal data and of different categories of data subjects,
    Art. 31 Time-limits for the storage and erasure of personal data,
    Art. 36 Right of access for the data subject,
    Art. 37 Right to rectification, erasure and restriction and,
    Art. 38 Responsibility in data protection matters.

100. As discussed in the previous paragraph arts. 49 and 50 ER contain the legal basis to claim compensation for damage from Europol.

---

[91] Judgment of 23 October 2024, *Keserű Művek Fegyvergyár Kft. v European Union represented by the European Commission*, T-519/23, ECLI:EU:T:2024:733; Also see judgement of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 135.

[92] Judgment of 13 December 2006, *É.R. and Others v Council and Commission*, T-138/03, EU:T:2006:390, par. 134; See further judgement of 17 December 2008, *Portela v Commission*, T-137/07, EU:T:2008:589, par. 80.

IV.3 Privacy and data protection in the Union

101. Privacy and data protection are fundamental aspects of the legal order of the European Union. This follows from the TFEU and the EU Charter. In this chapter the legal context of privacy and data protection in the Union is discussed as far as this is relevant to the Application and interpretation of the Europol Regulation.

102. On multiple occasions the CJEU has stressed the importance of a high level of protection for citizens where it concerns their privacy and data protection.

IV.3.1 Right to respect for private and family life

103. Art. 7 EU Charter provides that every individual in the EU has the right to respect for their private and family life, home, and communications. An interference with that right is only justified if it is provided by law, respects the essence of the rights, meets objectives of general interest recognised by the Union, and is necessary and proportionate (art. 52 EU Charter).

IV.3.2 Right to protection of personal data

104. Art. 16(1) TFEU and art. 8(1) EU Charter provide that everyone has the right to the protection of personal data concerning him or her. [93] This right is specific to the EU Charter, compared to for instance the European Convention of Human Rights, which underlines the importance that is attached to this right in the Union. Art. 8(2) EU Charter provides that personal data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. In addition, it lays down the right of everyone to access to data which has been collected concerning him or her, and the right to have it rectified. Europol is fully bound by these principles and must give full effect to the rights contained therein.

IV.3.3 Right to good administration and effective remedy

105. Art. 41 EU Charter provides for the right to good administration, which contains the right to have his or her affairs handled impartially, fairly and within reasonable time by an agency of the Union, right to have access to his or her file while respecting the legitimate interests of confidentiality and of professional and business secrecy and the obligation of the administration to give reasons for its decisions. Also of relevance is the right to an effective remedy (art. 47 EU Charter), which is intricately linked to the right to good administration but also to the right of access.[94]

106. The duty to take concrete measures to ensure respect for fundamental rights also follows from the EU Charter.[95] This is underlined by Europol's own code of conduct where it states:

> The nature of Europol as a European law enforcement agency delivering a public service requires EU citizens to have the confidence that Europol acts professionally, transparently and with integrity, in accordance with

---

93 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 15.

94 Decision EDPS, 8 September 2022, pars. 3.14 and 3.35 (**Annex A.2**).

95 Article 51 EU Charter.

fundamental rights, the right to good administration, as well as the public service principles for the EU civil service.[96]

107. Europol is thus held – under all circumstances – to take measures to ensure it complies with the duties resting upon it.

IV.3.4 EU data protection legislation

108. Within the EU legal system of data protection and the processing of personal data there are multiple regulations and directives that are of relevance for the interpretation of the right to privacy and right to data protection. Recital 40 ER provides that data protection rules at Europol should provide a "high level of protection of individuals with regard to the processing of personal data" and underlines that these rules must be "consistent with other relevant data protection instruments applicable in the area of police cooperation int he Union" and with the general principles underlying data protection in the EU.

109. To this end it is relevant to note that the Law Enforcement Directive (**LED)** introduced rules on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.[97] The LED addresses the competent authorities of Member States and while it is not applicable to the processing of personal data by EU agencies, such as Europol, the Europol Regulation does stress the importance of in particular this Directive.[98]

110. Furthermore, rules specific to the protection of natural persons with regard to the processing of personal data by the EU institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the European Union were established in Regulation 2018/1725 (**EUDPR**).[99] This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and it applies to the processing of personal data by all EU institutions and bodies.[100] Although this Regulation was not applicable to data processing by Europol at the time of the unlawful conduct, the principle of uniform and consistent interpretation within the Union makes that this regulation is relevant.[101]

111. The Europol Regulation, as mentioned, was thus shortly introduced after the GDPR and the LED. It provides an even more specific set of rights and obligations in this regard that apply specifically to data processing by Europol. Where uncertainty might rise as to the interpretation of certain provisions these other EU rules on data protection and privacy are of importance for a homogeneous interpretation of EU

---

96 Europol Code of Conduct, 5 December 2019, last accessed: 6 October 2025, URL: https://www.europol.europa.eu/sites/default/files/documents/the_code_of_conduct_of_europol.pdf, p.1.

97 Directive (EU) 2016/680 of 27 April 2016 Law Enforcement Directive (LED), entry into force: 5 May 2016, OJ L 119/89.

98 Article 2(3) LED; Recital 40 ER.

99 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018, OJ L 295/39.

100 Judgment of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 17.

101 In addition for the interrelation of Regulation (EU) 2018/1725 and the GDPR see judgement of 8 January 2025, *Bindl v European Commission*, T-354/22, ECLI:EU:T:2025:4, par. 18.

law in particular, the Law Enforcement Directive as it relates to the similar context of law enforcement.

V. THE UNLAWFUL CONDUCT, PLEAS IN LAW

V.1 Introduction

112. In this chapter six pleas in law are set out detailing that Europol violated its obligations under arts. 18(1), 18(2), 28(1), 30(2), 30(3), 31(1), 31(6), 36(1), 36(2), 36(4), 36(5), 36(6), 36(7), 37(1), 38(3), 38(4) and 40(1) ER and arts. 7, 8(1), 8(2), 41(1), 41(2) and 47 EU Charter. By and of itself, as well as a result of breaching its obligations, Europol thereby infringed the right to respect for private and family life, the right to the protection of personal data, the right of access to personal information, the right to rectification and erasure, the right to good administration and right to an effective remedy as defined in the ER and EU Charter.

113. The six pleas set out below are divided between Europol's acts and omissions. First, the infringement of Van der Linde's rights to privacy and data protection by failing to assess that the processing of Van der Linde's personal data was in accordance with Europol's objectives, i.e. whether it acted within its mandate, (Plea I) and by failing to process Van der Linde's data in accordance with the law (Plea II). Second, the infringement of Van der Linde's right of access to his personal information, right to rectification and erasure, right to good administration and right to an effective remedy, by failing to adequately handle his personal data access request (Plea III) and preventing him to exercise his corresponding rights (pleas IV, V and VI)).

114. Of importance to all six pleas is that the Europol Regulation is applicable. Van der Linde is a data subject as defined by the ER. The data that was shared by the Dutch authorities via SIENA message qualifies as "personal data" as it contained information relating to Van der Linde. The sending of this personal data to Europol via the SIENA message in 2018 by the Dutch Police qualifies as "transfer of personal data". Van der Linde's Twitter profile data that was contained on a mobile phone also qualifies as personal data. By sharing the phone with Europol and requesting on 7 February 2020 to extract data from it in the context of an ongoing Dutch investigation the Police transferred personal data to Europol. Europol's processing operation performed on the sensitive personal data included at least the following acts of Europol: collection, recording, organisation, structuring, storage, use, and restriction. Europol is the controller of Van der Linde's personal data it processed.

V.2 Pleas I-II: Europol infringed Van der Linde's rights to privacy and data protection

115. Pleas I and II both relate to privacy and data protection but differ in one significant aspect. Plea I is based on the fundamental argument that Europol – at all times – must act in accordance with and within the limits of its mandate. This creates a specific obligation for Europol to establish that the personal data it processes is warranted by its legally mandated objectives. Plea II corresponds to this as it is based on the argument that Europol, more broadly, must process personal data lawfully, and differs from it as it holds Europol jointly and severally liable for the unlawful data processing operation. As such Van der Linde needs not to specify in the context of an

unlawful data processing operation by Europol which unlawful conduct led to the damage he seeks compensation of.

V.2.1 Plea I: Europol unlawfully failed to establish whether processing Van der Linde's data fell within its mandate

116. Europol violated Van der Linde's right of data protection and right to respect for his private and family life as set out in arts. 7 and 8 EU Charter, by breaching its obligations as derived from arts. 18(1), 18(2) and 30(2) ER. The legal framework of the Europol Regulation establishes, as manifested by these provisions, an obligation for Europol to establish whether the personal data it processes is in accordance with its mandate and objectives. This simple rule – an EU agency may only use its vast and invasive powers within its strictly defined mandate – is a fundamental aspect of the rule of law and democratic societies. Europol violated this obligation when it did not assess whether the information, containing sensitive personal data of Van der Linde, it received from the Dutch Police could be processed in accordance with its objectives. Would Europol have made such an assessment it reasonably could only have concluded that the processing fell outside its mandate and thus would have had to reject Van der Linde's personal data, thereby preventing a violation of his fundamental rights. Europol does have a procedure to reject personal data shared by a Member State, as was disclosed to Van der Linde by Europol's Data Protection Function officer, but it did not make use of this procedure.

V.2.1.1 Europol's obligation to assess objectives and purposes (mandate)

117. The Europol Regulation sets out several obligations aimed at protecting the fundamental rights of individuals and is intended to confer rights on individuals. Ensuring respect for fundamental rights is a central element of the Europol's tasks, as demonstrated by, amongst others, Chapter VI ER on data protection safeguards.

118. The duty to take concrete measures to ensure respect for fundamental rights additionally emanates from art. 51 EU Charter, which is binding on Europol. Europol is thus held – under all circumstances – to take measures to ensure it complies with the duties resting upon it. The positive duty of Europol to strictly act in accordance with its objectives required that it takes measures to prevent fundamental rights violations. Furthermore, given the powers Europol is accorded under the Europol Regulation, it could and should have taken measures that could have reasonably been expected to prevent the infringement of the fundamental rights of Van der Linde.

119. The right to data protection and privacy applies to all European agencies and to Member States in their application of European law. All data processing operations of Europol should respect the right to data protection as protected in the EU Charter, the Europol Regulation, and the Law Enforcement Directive.

120. In particular, Europol's role as law enforcement authority makes that the right to the protection of the presumption of innocence tasks Europol with a general obligation, not to process information that do not fall within its mandate and if it needs to do so in the context of an operation, to label it adequately.

121. The obligation on Europol to assess whether the data it processes is in accordance with its mandate is cemented in arts. 18(1), 18(2) and 30(2) ER. **Art. 18(1)** concerning the states:

> 1. In so far as is necessary for the achievement of its objectives as laid down in Art. 3, Europol may process information, including personal data.

122. Art. 18 ER contains the obligation for Europol to assess whether the processing of personal data is necessary for the achievement of its objectives, i.e. whether it is in accordance with its mandate.

123. Furthermore, **art. 30(2)** ER limits the processing of sensitive personal data, such as political opinions and health status, to very exceptional situations:

> 2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life shall be prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol.

124. Art. 30(2) ER contains a prohibition for Europol to process sensitive personal data unless this is strictly necessary and proportionate to meet its objectives. This also requires Europol to make this assessment when processing such data.

125. Europol's objectives are laid out in art. 88 TFEU and were included in nearly identical terms in art. 3 ER. As detailed above, the objectives are the supporting and strengthening of action by Member States and their mutual cooperation "in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I" and "related criminal offences".

126. Arts. 18(1) and 30(2) ER are based on the understanding that Europol has an obligation to assess if processing is necessary and proportionate for the achievement of its objectives and would be rendered meaningless if this obligation would not exist.

127. In addition, **art. 18 (2)** ER further defines the objectives of Europol by limiting the processing of personal data to only four specific purposes. Part of the assessment in light of the objectives is also an assessment of whether the personal data being processed serves one of the limited purposes mentioned in art. 18(2) ER. Arts. 38(4) and 28(1) ER detail explicitly that Europol is responsible for compliance with the data protection principles that personal data shall be (a) processed fairly and lawfully, (b) collected for specified, explicit and legitimate purposes, (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, and (f) processed in a manner that ensures appropriate security of personal data. The importance of assessing the purpose of the processing follows clearly from these principles.

128. The four limited purposes of art. 18(2) ER for which Europol may process personal data are:

> (a) cross-checking aimed at identifying connections or other relevant links between information related to: (i) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence; (ii) persons

> regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent;
>
> (b) analyses of a strategic or thematic nature;
>
> (c) operational analyses;
>
> (d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.

129. These purposes thus provide further limits to Europol's mandate. Recital 43 ER underwrites the importance of, in the context of law enforcement cooperation, distinguishing between distinct categories of data subjects (for instance between suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses).

V.2.1.2 Obligation is evident in light of wording, context, and objectives of Europol Regulation

130. The obligation, as detailed above, is besides its unambiguous wording also apparent in light of the system and objectives of the Europol Regulation. Other articles supporting this understanding of arts. 18 and 30 ER are in particular arts. 7, 17, 18(6), 28(1), 29(4), 31 and 38 ER.

131. The CJEU held in the *Kočner/Europol* case that it is settled case-law that in order to interpret an article it is necessary "to consider not only their wording but also their context and the objectives pursued by the rules of which they are part".[102]

132. The legal basis to process personal data in order for Europol to comply with its obligation to assess whether it falls within its objectives and is for legitimate purposes is provided in art. 18(6). This provision makes explicit that Europol can temporarily process data specifically for the purpose of determining "whether such data are relevant to its tasks and, if so, for which of the purposes referred to in paragraph 2."

133. In addition, art. 17 ER concerning "sources of information" states that Europol "shall only process information that has been provided to it […] by Member States in accordance with their national law and article 7". This article cannot be understood as relieving Europol from its obligation under art. 18(1) ER and placing that burden on the Member State. This provision actually provides an independent obligation for Member States to provide information in compliance with their national law (arts. 17 and 7 ER) and that Member States are responsible for the legality of the data transfer to Europol (art. 38(5)(a) ER). Article 17 ER thus does not place an obligation on the Member State to assess the lawfulness of the data processed by Europol, but rather an obligation to ensure its own transfer of data to Europol is lawful.

134. Europol cannot outsource its obligation to make an assessment by simply requiring from Member States that to use the SIENA system they have to select a category for the data they transfer to guarantee that it can be processed within Europol's

[102] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 54, and referencing judgement of 3 June 2021, *TEAM POWER EUROPE*, C-784/19, EU:C:2021:427, par. 43.

mandate. This way of operating would also not be in conformity with art. 33 ER which requires data protection by design.

135. It must be noted that art. 19 ER concerning the "Determination of the purpose of, and restrictions on, the processing of information by Europol" states that Member States shall (also) determine the purpose for processing but this does not relieve Europol of its responsibilities as derived from arts. 18(2) and 38(4) ER. This is also evident from the fact that if a Member State does not determine the processing purpose, Europol still has to determine this (art. 19 ER).

136. Art. 28(1) ER further requires that all personal data be processed fairly and lawfully, not be further processed in a manner incompatible with specified, explicit and legitimate purposes, be relevant to what is necessary in relation to the purposes for which they are processed and be processed in a manner that ensures appropriate security of personal data. This article makes clear that Europol can only process personal data if its lawful and it is evident that this also requires an assessment of the purpose and objectives for which the processing takes place.

137. Art. 29(4) ER further states that Europol is to make an assessment of the reliability of the source and accuracy of information if a Member State does not do so. This article clarifies that Europol will always make an assessment of the data it receives, albeit for different purposes.

138. Art. 31 ER also builds on the assumption that an assessment has been made in respect of the objectives and purposes of data processed by Europol as it proscribes that personal data is not to be stored longer than necessary and proportionate for the purposes for which the data was processed.

139. Art. 38 ER relates to data protection matters and not grounds for processing. As mentioned, the responsibility for the quality of personal data as referred to art. 28(1)(d) ER, which state that personal data shall be accurate and kept up to date, shall lie with both the Member State or the Union body which provided the personal data to Europol, and with Europol in respect of personal data provided by third countries or international organisations or directly provided by private parties, or personal data retrieved by Europol from publicly available sources or resulting from Europol's own analyses; and of personal data stored by Europol in accordance with art. 31(5) ER. This latter requires an assessment of the information Europol processes. The first, which places the responsibility for accuracy of information on the Member State does, however, not relieve Europol from making an assessment of the information at hand. And if it does so and becomes aware that personal data provided by a Member State is factually incorrect or has been unlawfully stored then Europol has to act according to art. 38 (3) ER.

140. Lastly, a fundamental pillar of EU law is protection of fundamental rights. The Europol Regulation emphasises the protection of fundamental rights (i.e. privacy) of individuals and stresses the invasive risks of Europol's powers (which justifies high levels of protection). Recital 76 ER states that the Regulation respects the fundamental rights and observes the principles recognised in particular by the EU Charter, in particular the right to the protection of personal data and the right to privacy as protected by arts. 8 and 7 EU Charter, as well as by art. 16 TFEU. Negating

Europol's obligation to assess whether it acts in accordance with its objectives undermines the *effet utile* of the provisions safeguarding privacy and data protection.

141. It becomes clear from the above-mentioned provisions that the Europol Regulation places a clear and precise obligation on Europol. This obligation is detrimental to the lawful functioning of Europol.

V.2.1.3 Europol breached its obligation

142. From the facts of the case, it follows that Europol breached its obligation to only process data within its mandate and for the limited purpose listed. It failed to make a proper assessment to this end. Europol failed to provide any documentation in the investigation of the EDPS to even suggest it made a lawfulness assessment.

143. Europol has admitted via its DPF in a letter from 27 March 2025 to Van der Linde that there is a procedure to reject SIENA messages that do not fall within the objectives:

> "There is a procedure in place to reject SIENA messages not falling under the mandate of Europol."[103]

144. This indicates that Europol is able to make such an assessment and sees it as its responsibility to do so.

145. If Europol would have assessed the SIENA message it received on 29 May 2018 it reasonably could only have concluded that the personal data processing would fall outside its mandate. The SIENA message contains no information that could justify the label "Crime Area Terrorism". The core of the message focussed on Van der Linde moving to Berlin for medical treatment and the intention of stopping his social benefits. The Police explicitly mentions that it has no signals that Van der Linde would act violently or information that he had been violent in the past. The message was merely a "heads-up" about "a little concern". Processing this sensitive personal data clearly falls outside the objectives of Europol as it has no relation to preventing or combating terrorism, serious crime, crimes that could affect a common Union interest or even related crimes.

146. Europol's achievement of its objectives could in no way serve as a justification for the data processing of Van der Linde's sensitive personal data. This is obvious from the fact that Van der Linde did not commit any crimes, nor was he suspect of committing any by the Netherlands. The Police stated it continually stressed that in its SIENA message it was evident that Van der Linde was not violent or radical.[104] It also stated it had no reason to associate him with terrorism, and the Court has ruled that the Police and the NCTV did not have any justification to even qualify him as extremist.

147. It is reminded that the personal data processed contained information revealing his political activities, i.e. activism, and his leftwing political opinions, justifying even more caution and protection. Europol was not allowed, based on art. 30(2) ER, to process this sensitive data as it was not strictly necessary and proportionate to achieve Europol's objectives.

---

[103] E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025, p. 2 (**Annex A.23**).

[104] E-mail Police to Van der Linde re. intended appeal, 26 March 2025, p. 1 (**Annex A.20**).

148. The reason the Dutch Police linked Van der Linde to terrorism is that this was necessary to fill in the SIENA form:

> "There was no other choice [...] than to choose the field 'terrorism'. The other options relate more to forms of serious crime, such as organised crime, drug trafficking, money laundering, etc."[105]

149. From this fact alone, but especially in light of the stated intention of the Police in the SIENA message that it did not requested any action and that it was merely a heads-up, it is clear that the processing of this personal data could not serve the objectives of Europol or purposes of article 18(2) ER. Europol has not provided a purpose for which the data was processed. Regardless, it is evident that the data processing did and could not serve any of the purposes listed in the Europol Regulation.

150. In relation to art. 18(2)(a)(i) ER it cannot pose a justification as Van der Linde was not suspect of nor has he committed a criminal offence even merely related to the crimes within the competence of Europol. Similarly, (a)(ii) cannot pose a justification as there were and are no factual indications or reasonable grounds to believe that he will commit criminal offences in respect of which Europol is competent. The jurisprudence of the CJEU has made clear that law enforcement authorities cannot collect data of an individual without linking it to a criminal investigation.[106] Also the analyses of strategic or thematic nature or operational analyses, as mentioned in art. 18(2) b and c ER, provided no justified processing purpose. It remains without explanation, let alone justification, as to why his personal data was analysed in the operational analysis project AP Dolphin.

151. In relation to purpose (d), of facilitating exchange between Member States, it needs to be stressed that this can also not justify the processing by Europol. A distinction is made between, on the one hand, the process of sharing data between Member States via the SIENA system ("bilateral exchange of data using Europol's infrastructure between Member States […] to which Europol has no access") as referred to in art. 39(7) ER. And, on the other hand, the process of sharing data between Member States via SIENA to which Europol has direct access. In this case the Netherlands included Europol separately as a recipient of the data by sending a SIENA message to the German authorities and including Europol in the CC. Europol knew the content of that SIENA message. The processing of that data thus does not serve the purpose of facilitating bilateral exchange. It is not required for the exchange to take place to send it to Europol in CC. More specifically, Europol has not held that it processed the data to facilitate the exchange with Germany or any other Member State for that matter.

152. The only exception to Europol's obligation to assess personal data it processes in relation to its objectives and purposes is art. 38(7) ER which excludes Europol's responsibility in relation to bilateral exchange of data using Europol's infrastructure between Member States, Union bodies, third countries and international

---

[105] Decision Police (annulled) re. rectification SIENA messages, 31 January 2023, p. 3 (**Annex A.17**). Also see Decision Police (new), 29 September 2025, p. 2 (**Annex 21**).

[106] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (2014) C-293/12 and C-594/12, pars, 58-62

organisations to which Europol has no access. Evidently, this exception does not apply to this case.

153. Europol thus failed to assess whether the sensitive personal data it received from the Dutch Police could be processed within its mandate.

V.2.2 Plea II: Europol unlawfully processed Van der Linde's personal data

154. Europol also violated Van der Linde's right of data protection and right to respect for his private and family life as set out in arts. 7 and 8 EU Charter, by breaching its obligations derived from arts. 7 and 8 EU Charter and arts. 28(1), 30(2), 30(3), 38(3) and 38(4) ER. The Europol Regulation provides protection of personal data by establishing rules delineating how processing of personal data must occur. The processing of Van der Linde's personal data was not fairly and lawfully, nor collected for a specified, explicit, and legitimate purposes and not adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Would Europol have respected its obligations no violation of Van der Linde's rights would have occurred.

155. Van der Linde thus holds Europol jointly and severally liable for the unlawful data processing operation. It follows from art. 50(1) ER and the CJEU's jurisprudence (*Kočner/Europol*) that, if the harmful act is attributable to several entities, they are jointly and severally liable to compensate the damage.[107] In this instance both Europol and the Dutch Police took part in the unlawful data processing operation. Van der Linde is not required to argue exactly whether the police's or Europol's unlawful conduct resulted in the damage he incurred for Europol to be liable.

V.2.2.1 Europol breached its obligations

156. The facts of the case clearly demonstrate that Europol breached multiple the Europol Regulation obligations that impose limits on how the processing of personal data may be done by Europol.

157. Most far reaching in this regard is the obligation of art. 30(2) ER. As addressed in Plea I, the provision prohibits the processing of sensitive personal data revealing political opinions and an individual's health status. Europol breached this obligation as it processed exactly this type of sensitive personal data from the SIENA message and his Twitter profile, which reveal his political opinions and health status and the latter also his philosophical beliefs.

158. The SIENA message refers to his leftwing political views and that he is in therapy in Berlin, and the Twitter profile supposedly contained information on his political views as he uses this platform to share these views. Van der Linde asserts that this data processing cannot be justified as being strictly necessary and proportionate for preventing or combating crime that falls within Europol's objective, because, as was noted above, the data processing did not fall within Europol's objectives and furthermore it lacked any relation to preventing or combating crime. There is no beginning of evidence proposed by Europol as to why this processing would have been necessary or proportionate. Europol has also not asserted this was the case.

[107] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, pars. 56-62.

Europol therefore violated the prohibition to process sensitive personal data by processing Van der Linde's data without legal justification.

159. Van der Linde has grounds to believe that the executive director did not follow art. 30(3) ER as there is no information whatsoever to suggest that he authorised a limited number of Europol officials to have access to this sensitive information. On the contrary, the information was stored in EAS and multiple departments were contacted internally by Europol's DPF officer regarding this information after Van der Linde submitted a data request. Would article 30(3) ER have been respected the DPF would only have had to contact those limited officials, as opposed to him contacting anybody within the agency that might have had access to his personal data as he did.

160. Additionally, the data processing was not in accordance with art. 28(1) ER. Art. 28, read together with art. 38(4) ER, provides that Europol is responsible for the compliance with the general data protection principles that personal data shall be (a) processed fairly and lawfully, (b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes, and (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

161. First, as was concluded above under Plea I, Europol did not lawfully process the data of Van der Linde as it does not fall within its mandate nor was it for a legitimate purpose as provided for in art. 19 ER. Second, Europol has never indicated what purpose it had for processing Van der Linde's personal data. From the facts it becomes clear that Europol processed the data in relation to terrorism as the data was possibly used by different departments and projects focused on terrorism. Van der Linde can with certainty establish that there cannot have been a specified, explicit and legitimate purpose in that regard, as he was never convicted or suspected of committing a crime within the competence of Europol, or a so called related crime, and certainly not for anything related to terrorism or extremism. As mentioned, according to the Dutch Police this would have been apparent from the SIENA message as the content of the message makes no reference to terrorism. Europol nonetheless processed his data, specifically, in relation to terrorism. Third, if it is presumed that the processing purpose was related to terrorism Europol also breached its obligation by processing personal data that was not adequate, relevant, or even limited to what was necessary in relation to the purpose for which it was processed. The data contained no information of relevance in respect to terrorism, making the data not adequate or relevant to that purpose. Van der Linde concludes that Europol did not ensure compliance with the data protection principles.

162. In addition, Van der Linde asserts that Europol should have been aware that the information shared by the Dutch police was inaccurate. The SIENA message content could in no way provide a justification for the use of the label "Crime area Terrorism". Art. 38(2) ER places the responsibility for the quality of personal data (accurate and kept up to date), as referred to in art. 28(1)(d) ER, in principle on the Member State which provides the personal data to Europol. However, if Europol becomes aware of any issues regarding the quality it should have informed the provider of that information in accordance with art. 38(3) ER. As Europol was obliged to assess the

data in light of its objectives and processing purposes, it needed to take notice of the content of the data and thus would only have been able to reasonably conclude that the content of the message provided no factual basis for the terrorism label. This should have been flagged as an issue with the quality of the data. This simple, and according to the Dutch Police, obvious observation would have had to trigger Europol's obligation to contact the Dutch Police to clarify and if necessary, rectify the data it had received. Europol never did this.

163. Europol also failed to duly document the processing operation, as mandated by article 18(4) ER. This duty to document is necessary to make sure That Europol is processing data that is relevant to its objectives. There are strict restrictions on the processing of data for law enforcement purposes. Europol seemingly did not document that the processing of Van der Linde's personal data was complying with the data protection safeguards. It did not provide the EDPS with the relevant documentation to this end.

164. Europol also infringed arts. 7 and 8 EU Charter. Art. 8 EU Charter dictates that personal data must be processed fairly for specified purposes and with a legitimate basis laid down by law. As detailed above, this was not the case. The Europol Regulation states the specific processing purposes, none being applicable to the current case. In addition, the processing lacks a legitimate basis in law as, as discussed above, the processing falls outside the mandate of Europol. As the Europol Regulation only allows to process personal data within its objectives and for the specified purposes the processing regarding Van der Linde lacked a legal basis. Processing personal data, including sensitive data, without legal basis also led to an infringement of Van der Linde's right to privacy (art. 7 EU Charter). Both interferences with art. 7 and 8 EU Charter lack a justification by law, as Europol failed to assess its mandate and acted outside of its mandate. Van der Linde further holds that this interference was neither necessary nor proportional.

V.2.3 Conclusion Pleas I and II

165. In summary, Plea I details that Europol breached its obligation (arts. 18(1), 18(2) and 30(2) ER) to assess whether sensitive personal data it intends to process is in accordance with Europol's objectives and the limited purposes provided for by the Regulation, thereby violating Van der Linde's right of data protection and right to respect for his private and family life as set out in arts. 7 and 8 EU Charter.

166. Plea II provides that in the unlawful data processing operation Europol breached its obligations (arts. 28(1), 30(2), 30(3), 38(3) and 38(4) ER and arts. 7 and 8 EU Charter) to not process sensitive personal data and comply with the data protection principles and arts. 7 and 8 EU Charter. Thereby it violated Van der Linde's right of data protection and right to respect for his private and family life as set out in arts. 7 and 8 EU Charter.

V.3 Pleas III-VI: Europol infringed on Van der Linde's rights of access to his personal information and to good administration

167. Pleas III-VI all relate to the handling by Europol of Van der Linde's access request to his personal information. Plea III concerns the unlawful rejection by Europol of this

request. Plea IV addresses the consequence of this rejection by which Europol unlawfully prevented Van der Linde to exercise his right to rectification and erasure. Plea V details the unlawful deletion by Europol of his personal data and Plea VI deals with how Europol frustrated the practical effect of the right of access to personal data.

168. The violations of Van der Linde's rights as detailed in these pleas constitute independent unlawful conduct of Europol. Van der Linde holds Europol liable for this conduct based on arts. 49(3) and 50(1) ER.

V.3.1 Plea III: Europol unlawfully rejected Van der Linde's data access request

169. Europol violated Van der Linde's right to obtain information on whether personal data related to him was processed by Europol and the right to good administration (arts. 8(2) and 41(2b) EU Charter and art. 36 ER) thereby breaching its obligations as set out in arts. 36(1), 36(2), 36(4), 36(5), 36(6), 36(7) and 40(1) ER and art. 41 EU Charter.

170. Europol did so by rejecting Van der Linde's data access request on 11 June 2020 which he had filed on 11 February 2020, and which Europol confirmed receipt of on 10 March 2020. In its rejection decision Europol stated: "there are no data concerning you at Europol to which you are entitled to have access in accordance with Art. 36 of the Europol Regulation."[108]

171. As the EDPS found in its decision of 8 September 2022 on Van der Linde's complaint against this rejection (i) Europol failed to provide all information he had a right to receive; (ii) Europol's refusal was insufficiently motivated, (iii) Europol wrongly referred the handling of a part of his request to the Netherlands; (iv) Europol potentially wrongly deleted personal information relating to Van der Linde pending the EDPS investigation.[109]

V.3.1.1 Europol violated right of access

172. The decision of the EDPS gives a detailed account of the unlawful conduct of Europol in answering van der Linde's request. Europol's response to the access request of Van der Linde was, according to the EDPS, inadequate as Europol did not sufficiently motivate its decision and failed to document internally the legal and factual reasons for this decision.[110] Europol also violated the right of Van der Linde to obtain reasons for the refusal of his access request and failed to adequately document the refusal decision.

173. First, Europol violated Van der Linde's right to request access to his personal data as laid down in art. 36 (1). Europol rejected his data access request altogether and its response was insufficient. By merely stating that there was no data concerning Van der Linde at Europol to which he was entitled to have access to, Europol did not respond adequately and sufficiently clear to the request. On the one hand it leaves open the possibility that Europol has not processed personal data of Van der Linde by not explicitly stating that and on the other hand it also leaves open the possibility

---

[108] Decision Europol refusing data access, 11 June 2020 (**Annex A.25**).
[109] Decision EDPS, 8 September 2022, pars. 3.58-3.60 (**Annex A.2**).
[110] Decision EDPS, 8 September 2022, par. 3.59 (**Annex A.2**).

that it did process information but that Van der Linde could not have access to it. But by failing to provide any reason, as Europol was obliged to, Van der Linde could not know for certain what was meant by the answer of Europol. This ambiguity can best be understood in light of the facts that emerged by the EDPS investigation, namely (i) that before rejecting the request Europol possessed at least two items of personal data, (ii) Europol subsequently deleted this data before the rejection and (iii) it turned out that Europol in fact did not erase the data but retained it instead in its archive, meaning it is still in its possession.

174. Furthermore, none of the information that Europol was required to provide to Van der Linde, based on art. 36(2) ER, was provide to him.[111] In clear violation thereof Europol failed to (a) confirm whether or not data related to him was being processed, (b) inform him on the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data was disclosed, (c) communicate the data undergoing processing and of any available information as to their sources, (d) indicate the legal basis for processing the data, (e) inform him on the envisaged period for which the personal data would be stored and (f) inform him on the existence of the right to request from Europol rectification, erasure or restriction of processing of personal data concerning him.

175. The only exception to deny access follows from art. 36(6) ER which states that access may be refused or restricted if such refusal or restriction constitutes a measure that is necessary in order to: (a) enable Europol to fulfil its tasks properly; (b) protect security and public order or prevent crime; (c) guarantee that any national investigation will not be jeopardised; or (d) protect the rights and freedoms of third parties. Art. 36(6) ER explicitly adds that when the applicability of an exemption is assessed, the fundamental rights and interests of the data subject shall be taken into account.

176. None of these refusal grounds were communicated by Europol to Van der Linde at the time of rejecting the request and none of them justify refusing the request. In its response Europol only referred to arts. 36 and 37 ER in general as ground for refusing access.

177. Only after the EDPS started its investigation did it became known that the DPF had recommended to refuse access to Van der Linde based on art. 36(6)(a) ER.[112] It remains unclear if this recommendation was followed and was relied on by Europol. Regardless, it is evident that the use of this ground for refusal is unwarranted. If Europol's use of this ground would be accepted it would deprive the right to access of its meaning and practical effect. Without any concrete justification as to why granting access to Van der Linde would jeopardize Europol to fulfil its tasks properly, and thus make it necessary to restrict access, or even refuse it, this argument has to be rejected. This exception can thus not be relied upon as justification to no comply with art. 36(2) ER.

178. Even more striking is that Europol needed to produce a perceived justification only after AP Dolphin, as it informed the DPF on 28 May 2020, had already deleted the

---

[111] See to that effect Decision Europol refusing data access, 11 June 2020 (**Annex A.25**).

[112] Decision EDPS, 8 September 2022, par. 2.10 (**Annex A.2)**.

data from the SIENA messages.[113] This did not happen once but twice. After the DPF went to check whether the data was actually deleted it discovered that the Twitter profile data was also stored in EAS. On 5 June 2020, the ECTC responded to Europol's request that the Twitter account "was not relevant from an operational point of view and could be deleted from EAS".[114] And subsequently it deleted this information as well.[115] Internally Europol did not see any justification for the refusal of access to this data, but nonetheless it did prevent Van der Linde to get access, because it had deleted his personal data.

179. In a twisted, and clearly illegal way, the refusal could be perceived as necessary for Europol to fulfil its tasks properly, because granting access seemed to have become impossible after deleting the data it had to provide access to. This conduct is brazenly in violation of art. 36 ER.

180. Even though art. 36(6) cannot be invoked in any convincing way by Europol it is noted here that art. 36(7) provides a ground for Europol to not share information on the reasons for the refusal of a request "where the provision of such information would deprive paragraph 6 of its effect". At no point did Europol express that it relied on this paragraph to not provide reasons to Van der Linde. There is also no conceivable reason as to why paragraph 6 would be deprived of its effect by specifying that Van der Linde's request would be refused because other than covering up the fact that it had deleted his data pending his request. Art. 36(7) ER furthermore specifies that Europol shall in any case notify the data subject that it has conducted the required checks, without giving any information which might reveal whether or not personal data was processed by Europol. The general reference to art. 36 and the use of the word 'checks' in its rejection was misleading as this leads one to believe that there is a legal justification based in arts. 36(6) and (7) to not receive more information while this was in fact not the case.

181. Furthermore, Europol did not comply with art. 36(5). This provision states that Europol shall consult the competent authorities of the Member States and the provider of the data concerned on a decision to be taken. This is not what Europol did. It simply requested if the Dutch competent authority would agree to the release of information to Van der Linde.[116] There is no evidence to suggest that Europol independently formulated its intended decision, let alone communicated this intended decision to the Netherlands. The message that was sent to the Dutch Liaison Bureau does not provide a basis to argue Europol's intended decision was to grant access. On the contrary, as emerged later, AP Dolphin internally already proposed to delete the data.

182. A proper consultation with the Netherlands on a clearly formulated intended decision would have required a different response from the Netherlands. It is evident that in that situation the Netherlands would not have been able to propose that deleting the information could be a solution to the problem, as it did in its response. A genuine consultation is a safeguard to guarantee the right of access to information. Both the

---

[113] Decision EDPS, 8 September 2022, par. 2.7 (**Annex A.2)**.
[114] Decision EDPS, 8 September 2022, par. 2.9 (**Annex A.2)**.
[115] Decision EDPS, 8 September 2022, par. 2.9 (**Annex A.2)**.
[116] Decision EDPS, 8 September 2022, par. 2.6 (**Annex A.2**).

Member State and Europol should hold each other to account. By not respecting this process Europol also failed to respect Van der Linde's right of access.

183. In addition, Europol also violated art. 36(4) because it did not respond to Van der Linde's request without undue delay. Van der Linde submitted his request directly to Europol on 11 February 2020 and Europol also received the request via the Dutch Police on 10 March 2020. The rejection was sent on 11 June 2020. This is 4 months later than Van der Linde's initial request, which cannot be considered to be sent without undue delay.

184. Finally, Europol also violated art. 40(1) ER. This provision requires Europol for the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data integrity and security, to keep records of the collection, alteration, access, disclosure, combination, or erasure of personal data. This logging of information is essential to give the right of access to information practical effect. Without this obligation it would be difficult, if not impossible, for Europol to meet its obligations of art. 36, as displayed by the difficulties the DPF had to internally trace "the origin and relevance of the information on the complainant's Twitter account".[117] Van der Linde can only conclude that Europol did not keep proper records of the above processing. Additionally, it is noted that this issue was not (sufficiently) addressed by the EDPS and this was therefore a reason for it to decide to review its decision and investigate the alleged lack of a documented assessment of the lawfulness of processing of Van der Linde's personal data by Europol.[118] Van der Linde also asserts that this lack of documented assessment of lawfulness leads to a violation of art. 40 (1) ER.

V.3.1.2 Europol violated right to good administration

185. The facts, as detailed above, also lead to the conclusion that Europol violated the right to good administration (41 EU Charter). This right entails that Van der Linde has the right to have his affairs handled impartially, fairly and within a reasonable time by Europol (art. 41(1) EU Charter). More specifically it entails that Van der Linde has the right to have access to his file, while respecting the legitimate interests of confidentiality and of professional and business secrecy (art. 41(2a) EU Charter) and that Europol has the obligation to give reasons for its decisions (art. 41(2b) EU Charter).

186. Europol has not handled Van der Linde's request impartially or fairly as it follows from the facts that both Europol and the Netherlands were seeking reasons to limit his access, and this resulted in Europol deleting data to which he had requested access. Europol's handling further shows a clear bias against Van der Linde and Europol acted in bad faith by deleting his data on two occasions. Again, its decision was not given in a reasonable time as it surpassed the period defined in the Europol Regulation. As discussed above Europol has, in this case, also no claim of legitimate interests of confidentiality. Europol, furthermore, failed to provide reasons for its decision. This all leads to the inevitable conclusion that Europol violated Van der Linde's right to good administration.

---

[117] Decision EDPS, 8 September 2022, par. 2.8 (**Annex A.2**).

[118] Decision review EDPS, 30 January 2023, pp. 1-2 (**Annex A.29**).

V.3.2 Plea IV: Europol unlawfully prevented Van der Linde to exercise his right to rectification and erasure

187. The infringement of Van der Linde's right of access to personal information, as detailed above, also directly resulted in Van der Linde not being able to exercise his corresponding fundamental rights such as the right to rectification (art. 8(2) EU Charter and art. 37 ER) and the right to erasure (art. 37 ER) in a timely manner. The right of access to information is a necessary precondition to effectively exercise these rights.[119] Europol, by unlawfully rejecting Van der Linde's access request, precluded him from exercising his right to rectification and erasure. Had Van der Linde been able to exercise these rights, if Europol had not rejected his request in June 2020, this would reasonably have limited his damage. By not being able to do so he incurred further damages.

188. Only by the intervention of the EDPS might Van der Linde possibly be brought in a position again to exercise those rights. The EDPS ordered Europol that it should retrieve the deleted information,[120] after Europol stated that it had deleted all information (again). Currently, Europol indicated that Van der Linde's personal data was secured and independently stored for purposes of his access request procedure.[121] Even if this is the case and Van der Linde is able to request the erasure or rectification of his personal data, this does not mean that the damage that was inflicted since this right was violated can be undone.

189. Art. 8(2) EU Charter includes also contains the right to have the data rectified. Art. 37 ER further specifies the rights to rectification and erasure in the context of data access of personal data processed by Europol. The first paragraph states that a data subject has the right to request Europol to rectify personal data concerning him or her held by Europol if they are incorrect or to complete or update them. Paragraph 2 grants the data subject the right to request Europol to erase personal data relating to him or her held by Europol if they are no longer required for the purposes for which they are collected or are further processed. Furthermore paragraph 5 provides that if personal data held by Europol has been provided by a Member State, this Member State shall rectify or erase the data in collaboration with Europol, within their respective competences.

190. It is obvious that the personal data of Van der Linde, as shared in the SIENA message associating him with terrorism, is incorrect. This would have warranted a rectification and reasonably could only have led to the outcome, in case his right of access had been respected, that Europol would have had to rectify this data in collaboration with the Dutch authorities. Concerning the Twitter profile data Van der Linde is not in a position to assess whether the data is correct as Europol violated his right of access to it. Additionally, erasure would nonetheless also have been warranted for the Twitter profile data, as Van der Linde has detailed above, because there was no legitimate purpose for which the data was collected and further processed in the first place.

---

[119] Judgment of 17 July 2014, *YS and others*, C-141/12 and C-372/12, EU:C:2014:2081, par. 57.

[120] Decision EDPS, 8 September 2022, pars. 3.57, 4.1 and 4.2 (**Annex A.2**).

[121] Letter Europol to Van der Linde, 3 February 2025 (**Annex A.27**).

V.3.3 Plea V: Europol unlawfully deleted and retained Van der Linde's personal data

191. Europol breached its obligation to only store Van der Linde's data as long as this was necessary and proportionate as set out in art. 31(1) ER. Subsequently, it also breached its obligation to not erase personal data if this would damage the interests of a data subject who requires protection as set out in art. 31(6) ER.

192. Art. 31(1) ER determines that personal data processed by Europol shall be stored by Europol only for as long as is necessary and proportionate for the purposes for which the data are processed. A review of this shall occur no later than after three years of initial processing.

193. Europol should not have stored the SIENA message as long as it did. It received the sensitive personal data on 29 May 2018. There was no necessity to store this information for multiple years until 2020. The Dutch police thought so too, since it later cancelled the message, but failed to properly inform Europol of this.

194. Art. 31(6) ER specifies that personal data shall not be erased if this would damage the interests of a data subject who requires protection, in which case, the data shall be used only with the express and written consent of the data subject.

195. After Van der Linde requested access to his data, Europol proceeded to delete his data. At this point it was evident that deletion would severely damage the interests of Van der Linde as this would mean he could not exercise his right of access to it nor in that way find out who else might have received the information and try to limit his damage. Europol therefore had an obligation not to delete his data, even though it did already store it for too long. Paragraph 6 supersedes paragraph 1 once Van der Linde made his access request. Europol did not deleted his information once, but also on a second occasion when it discovered the data from the Twitter profile.

196. During the EDPS investigation, it turned out that Europol did not in fact do a hard deletion of the data. During EDPS' visit, Europol explained to the EDPS how it was possible to still retrieve this data despite having deleted it previously. With regards to Van der Linde's Twitter account, Europol explained that this could be found "via a targeted search in the EAS because this personal data was still stored in the raw document extracted from the mobile phone".[122] With regards to the SIENA messages, "Europol explained that the set of data related to the case will only be deleted when a new data retention functionality […] is implemented".[123]

197. Furthermore, Europol stated for a third time it deleted the data during the EDPS investigation. The EDPS has indicated that in case Europol had permanently erased the information stored about Van der Linde and not simply archived it, this would constitute a failure to cooperate with the EDPS and a serious infringement of the Europol regulation.[124] The EDPS concluded that Europol retains and stores copies of deleted data in its archives for a period of five years.[125]

---

[122] Decision EDPS, 8 September 2022, par. 2.20 (**Annex A.2**)
[123] Decision EDPS, 8 September 2022, par. 2.20 (**Annex A.2**).
[124] Decision EDPS, 8 September 2022, par. 3.50 (**Annex A.2**).
[125] Decision EDPS, 8 September 2022, par. 3.55 (**Annex A.2**).

198. This leads to the bizarre conclusion that Europol deleted the personal data of Van der Linde on multiple occasions but did not erase it. Each of these acts are in breach of art. 31(6) ER as this would clearly damage his interests and it did. Furthermore, the fact that it does not really erases personal data when it states it deletes the data is in violation of art. 31 ER.

V.3.4 Plea VI: Europol unlawfully frustrated the practical effect of the right of access to personal data

199. The inevitable conclusion, overseeing all the facts detailed above, is that Europol frustrated the practical effect of the right of access to personal data consistently throughout Van der Linde's access request procedure and the subsequent EDPS investigation. This is a violation of Van der Linde's right to good administration as set out in art. 41 EU Charter and right to an effective remedy as set out in art. 47 EU Charter.[126]

200. The CJEU has explained that the right to an effective remedy in the context of a refusal of access to a file by a law enforcement authority requires it to make available to the judicial authority the verification of the lawfulness of the processing of the data at issue as well as the conclusions which it drew from that verification.[127]

201. First, Europol decided on the rejection of his data request after an unduly long time. It did so while in the meantime colluding with the Dutch authorities to delete the data that was subject of the data access request. The rejection decision was misleading by creating the suggestion that there was a legal justification for not providing any reasons for its decision. Europol, in addition, misinformed the EDPS during its investigation, delayed the EDPS procedure as a whole, and failed to provide all the relevant information on time. Without any good reason Europol shared relevant information only after the EPDS made its decision. It also stated to the EDPS to have deleted the data that was subject to the investigation, which in itself was a gross violation of the Europol Regulation, but this turned out to be false information seemingly to reassure the EDPS. All this leads to a pattern of bad faith behaviour on behalf of Europol. At each crossroad Europol seems to have tried if it could get away with not fully respecting Van der Linde's rights, and when confronted with this it looked for different ways to frustrate the full exercise of his rights. In doing so Europol frustrated the practical effect of the right to access to information.

V.3.5 Conclusion Pleas III to VI

202. In summary, Plea III details that Europol breached its obligations (arts. 36 and 40(1) ER and art. 41 EU Charter), thereby violating Van der Linde's right to obtain information on whether personal data related to him was processed by Europol and his right to good administration.

---

[126] See for instance Judgement 16t November 2023, Ligue des droits humains ASBL, BA v Organe de contrôle de l'information policière, C-333/22, par. 58.

[127] Judgement of 16 November 2023, Ligue des droits humains ASBL, BA v Organe de contrôle de l'information policière, C-333/22, par. 69.

203. Plea IV provides that Europol violated Van der Linde's right to rectification and erasure as set out in art. 37(1) ER and his right rectification as set out in 8(2) EU Charter, in contradiction of Europol's obligations to respect these rights.

204. Plea V discusses that Europol breached its obligation (arts. 31(1) and 31(6) ER) to store personal data only for as long as necessary and proportionate and the obligation not to erase personal data once it is clear this would damage the interests of Van der Linde which required protection.

205. Lastly, Plea VI concludes that the ensemble of breaches of Europol's obligations as detailed above leads to a violation of Van der Linde's right to good administration as set out in art. 41 EU Charter and right to an effective remedy as set out in art. 47 EU Charter.

V.4 Rules that confer rights on individuals

206. It can be concluded from Pleas I-VI that the obligations, as discussed in above, confer rights on individuals, namely the rights as specified in arts. 7, 8, 41 and 47 EU Charter and arts. 36 and 37 ER and those implicitly conferred on individuals by the obligations of the Europol Regulation.

207. The failure of Europol to comply with these obligations constitutes a breach of rules of law intended to confer rights on individuals, in this case the rights of Van der Linde.

208. The requirement that the rule of law that is breached confers rights on individuals is fulfilled. Firstly, this is the case because the unlawful conduct and omissions by Europol set out in Pleas I-VI constituted a direct violation of Van der Linde's (fundamental) rights. Secondly, it is because the obligations breached by Europol are all aimed at protecting the (fundamental) rights of Van der Linde, albeit some more explicitly than others. Thirdly, the CJEU established that the obligation to protect individuals against the unlawful processing of their personal data based on the combined reading of Europol Regulation provisions constitutes of a rule of EU law intended to confer rights on individuals.[128] The CJEU has recognized that fundamental rights laid down in the EU Charter are rules of law intended to confer rights on individuals.[129] As set out above, the way the Europol handled Van der Linde's request violated those rights.

209. In sum, the rule of law breached, more specifically, the obligations and rights violated, by Europol, all confer rights on individuals relevant to Van der Linde's pleas in law.

V.5 Sufficiently serious breach of law

210. The violation of the aforementioned obligations by Europol resulted in a sufficiently serious breach of law. As determined in settled case-law of the CJEU, there is a sufficiently serious breach when the institution concerned manifestly and gravely disregarded the limits of its discretion. The factors to be taken into consideration in

---

[128] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 123.

[129] See for example judgement of 20 September 2016, *Ledra Advertising v. Commission and ECB*, C-8/15 P to C-10/15 P, EU:C:2016:701, pars. 66-67.

that connection being, inter alia, the degree of clarity and precision of the rule breached, and the measure of discretion left by that rule to the EU authorities.[130]

211. The facts of the case support the conclusion that there is a sufficiently seriously breach of the rule of law, as Europol violated Van der Linde's rights as set out in Pleas I-VI. The EDPS established with its decision the seriousness of the breaches it investigated.

212. It is evident that Europol acting in violation of its mandate is an extraordinary serious breach of law. Inherent to Europol's existence is that it acts in accordance with its mandate and thus has no discretion at all to not do so.

213. Also, the unlawful data processing operation proves to be a serious breach of law. Of direct relevance in this regard is the consideration of the CJEU in *Kočner/Europol* that arts. 28 and 38 ER do not leave Europol and the Member State involved in cooperation under that Regulation any discretion as regards their obligation to protect any individual against any unlawful form of making personal data concerning him or her available by implementing appropriate technical and organisational measures for that purpose.[131] The CJEU further held that this obligation forms part of the sensitive context of cooperation between Europol and the Member States for the purposes of criminal prosecution, in which such data are processed without any intervention by the data subjects, most often without their knowledge, and therefore without them being able to intervene in any way in order to prevent any unlawful processing of their data. [132] The CJEU gave significance to the intimate nature of the data which required strictly ensuring data protection.[133] It concluded that the unlawful processing of data in that instance was a sufficiently serious breach of a rule of EU law (art. 28 and 38) intended to confer rights on individuals.[134] The same holds for the current case, which concerns sensitive personal data outside the context of a criminal case.

214. The breach of the right of access and good administration and effective remedy are equally serious breaches. All concern fundamental rights that leave no, to very little, discretion to Europol. As discussed, the respective exceptions do not apply in this case which left Europol with no discretion in respect of observing these rights.

215. For all of the breaches discussed it must be stressed that the wrongful association with terrorism is a very hefty factor in the seriousness of the breach. In addition, that Europol seemingly acted in bad faith also increases the seriousness.

216. Based on the above, Van der Linde thus seeks compensation for the infringement of his rights to privacy and data protection as a result of the unlawful data processing operation (Pleas I and II) based on art. 50(1) ER. In addition, he also seeks

---

[130] See for example judgement of 5 March 1996, *Brasserie du Pêcheur and Factortame*, C-46/93 and C-48/93, EU:C:1996:79, pars. 55-56; Judgment of 25 January 2007, *Robins and Others*, C-278/05, EU:C:2007:56, par. 70; Judgment of 19 June 2014, *Specht and Others*, C-501/12 to C-506/12, C-540/12 and C-541/12, EU:C:2014:2005, par. 102; See Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 117.

[131] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 129.

[132] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 129.

[133] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 130.

[134] Judgment of 5 March 2024, *Kočner/Europol*, C-755/21 P, EU:C:2024:202, par. 131.

compensation for the infringement of his right of access to his personal data and the right to good administration as a result of the unlawful handling of his data access request (Pleas III-VI) based on art. 49(3) ER.

VI. DAMAGE

217. The damage that Van der Linde suffered as a direct result of the unlawful conduct set out in Pleas I-VI is actual and certain and consists of material and non-material damage.

218. Europol's infringement of Van der Linde's rights to privacy and data protection by failing to assess whether the data it processed was in accordance with its mandate and by unlawfully processing his personal data, and also Europol's infringement of his right of access to his personal information by unlawfully rejecting his request to access to his personal data, unlawfully preventing him to exercise his other fundamental rights, unlawfully deleting and archiving his personal data and unlawfully frustrating the practical effect of his right of access resulted in the following damage.

219. It is evident that the unlawful conduct was capable of causing non-material damage as detailed below and it did so in fact.

220. First, Van der Linde has suffered damage to his mental and physical health. His health seriously deteriorated as a direct result of finding out that Europol processed his personal data whilst associating him with terrorism and the subsequent treatment by Europol of his data access request. He has incurred mental injury in the form of trauma, and he has been diagnosed with PTSD as a result of the yearslong targeting and unlawful treatment by government and law enforcement authorities. Europol's unlawful conduct directly led to re-traumatisation on multiple occasions. Additionally, he suffered and suffers from panic attacks and insomnia that are triggered by the unlawful conduct of Europol (**Annex A.32**).[135] He has consulted his doctor continuously throughout his proceedings regarding the effects on his physical and mental wellbeing (**Annex A.33**).[136] His doctor has actually prescribed long term and regular trauma therapy outside of the Netherlands to prevent further deterioration of his mental health, as most triggers with negative consequences are situated in the Netherlands including Europol (**Annex A.34**).[137]

221. Second, Van der Linde suffers non-material damage because he has developed a profound anxiety as to what the consequences are of him being associated with terrorism by Europol. This fear is fed by (permanent) uncertainty about what the unlawful conduct of Europol might still lead to in the future, since he does not know to the full extent of who might have accessed his personal data or with whom Europol shared this data. This fear is omnipresent in his life, but it is especially prevalent when he travels abroad, which he regularly does on medical advice precisely to improve his mental wellbeing. His fear consists of, among other things, that he will be detained unlawfully and even pre-emptively while traveling abroad.

---

[135] E-mail Van der Linde re. trauma and panic attacks, 7 March 2022 (**Annex A.32**).
[136] E-mail Van der Linde to GP Van der Cingel, 7 April 2025 (**Annex A.33**).
[137] Letter GP Van der Cingel, 10 December 2021 (**Annex A.34**).

222. That risks exist for Van der Linde if he travels abroad, due to his personal data being processed by Europol in relation to terrorism, has been confirmed by the Mayor of Amsterdam (Femke Halsema), and the chief public prosecutor of Amsterdam (René de Beukelaer) in conversations with him. In addition, the former Dutch member of the European Parliament, Sophie in 't Veld, confirmed to him that this might be a very real danger to him (**Annex A.35**).[138] On separate occasions this fear has already manifested itself while traveling abroad. On multiple occasions he encountered issues, such as being submitted to an interview by border police *after* having passed security and customs or being escorted by a police officer until he boarded his plane (**Annex A.36**).[139] He did not previously encounter these types of issues while traveling. His fear is real, realistic, and serious and has resulted in non-material damage.

223. Van der Linde's realistic fear that his personal data has been shared with other parties is also rooted in an understanding of Europol's operations. For instance, art. 4 ER determines as one of the core tasks of Europol to "notify the Member States […] without delay of any information and connections between criminal offences concerning them". This makes it plausible that Europol has shared Van der Linde's personal data since May 2018 and that it did so with other Member States. Similarly, art. 20 ER, which determines the access by Member States and Europol's staff to information stored by Europol, justifies the fear of Van der Linde that other entities, still unknown to him, might have had access to his personal data and even might have processed it themselves. Arts. 22 and 23 ER are also relevant in this regard. Specifically, art. 23 ER which creates the possibility to share personal data even with third states. Uncertainty regarding who has had access to his personal data that was processed by Europol is a direct consequence of how Europol unlawfully handled his data access request.

224. Third, Van der Linde has suffered non-material damage because of the actions of Europol since his fundamental rights have been violated and consequently his human dignity and personal integrity have been harmed. The extent and way his fundamental rights have been violated resulted in non-material damage to him. He is aghast by the way he has been treated by Europol and the way in which his fundamental rights were disregarded. His reputation has been damaged.

225. Besides the non-material damage, Europol's conduct also caused material damage. Primarily, because he has been forced to spend a significant amount of his time and effort (more than 200 hours), at least since 2019, to contest Europol's incorrect and unlawful handling of his data access request and the subsequent treatment by Europol in this matter. As a self-employed person he was not able work and generate an income during the hours he spent on seeking justice. In addition, he has incurred legal costs in his process of seeking justice for the violations by Europol of his rights.

226. As a result of Europol's unlawful conduct, the extent of the consequences is not fully known (yet) to Van der Linde or might even never become (fully) known. This also

---

[138] E-mail Van der Linde to former lawyer re. serious risk of Europol terrorism association, 4 February 2022 (**Annex A.35**).

[139] E-mail Van der Linde to Mayor of Amsterdam and Municipal Secretary re. travel issues, 6 February 2025 (**Annex A.36**).

has implications for his damage. First, this uncertainty contributes to his damage as he suffers from an uncertain situation and is afraid his personal data might be shared with others while he is not able to correct that wrongful information. Second, it also affects the total amount of his damage as the full extent of it is not known (yet) to him. There is a real possibility that as more information comes to light about Europol's unlawful conduct, he discovers he has suffered and suffers additional damage.

227. The above-described damage amounts to, as currently known to him, €50.000 in non-material damage and €26.250 in material damage. In total this amounts to €76.250. Van der Linde has sufficiently established and proven this damage.

VII. CAUSAL LINK

228. There is a direct and certain causal link between Europol's unlawful conduct set out in Pleas I-VI resulting in a sufficiently serious breach of the rule of law intended to confer rights on Van der Linde and the damage suffered by him.

229. In relation to the unlawful failing to establish whether processing Van der Linde's personal data fell within its mandate (Plea I) both the material and non-material damage was caused by this conduct/omission. Would Europol have acted in accordance with its obligations it could reasonably only have concluded that the personal data processed contained no factual basis to justify the processing to prevent or combat terrorism and that it lacked a factual basis to serve one of the limited processing purposes. The Dutch police itself stressed that it did not associate Van der Linde with terrorism in the content of the message and that it selected the field "Crime area Terrorism" because it considered there not to be an alternative. In other words, Europol would have had to reject the processing of his personal data as it clearly fell outside its mandate.

230. The unlawful processing operation on Van der Linde's data (Plea II) is also in a causal connection to Van der Linde's damage. Although the unlawful conduct detailed in Plea I preceded the unlawful conduct detailed in Plea II, this does not negate the causal link between both these sets of unlawful conduct to the damage inflicted. The violated provisions of the Europol Regulation, as discussed above, contain important safeguards to prevent unlawful data processing. By violating these provisions, Europol subverted these safeguards which resulted in the damage. Would Europol have respected these articles this would have prevented the damage to occur to the extent it did.

231. The unlawful rejection of Van der Linde's data access request, the ensuing unlawful prevention of exercising his fundamental rights to erasure and rectification, the unlawful deletion of his personal data and the unlawful frustration of the practical effect of his right of access are all in a causal connection to the damage caused (Pleas III-VI). These unlawful acts resulted in additional and separate damage of Van der Linde. Learning of Europol's unlawful handling of his access request resulted in a further deterioration of his mental and physical health. In addition, it also resulted in material damage mentioned above as he had to spend significant efforts in response to set right the effects of the unlawful conduct.

232. That the Netherlands also acted unlawfully does not preclude that Europol's unlawful conduct was de direct and definite cause of the damage Van der Linde has suffered.

VIII. CONCLUSION AND ORDER SOUGHT

233. As has been set out above, by unlawfully processing Van der Linde's data, independently and as part of an unlawful data processing operation, Europol has seriously breached its obligations derived from arts. 18(1), 18(2), 28(1), 30(2). 30(3), 38(3) and 38(4) ER and arts. 7 and 8 EU Charter and therewith violated Van der Linde's rights under arts. 7 and 8 EU Charter. Furthermore, the unlawful conduct of Europol in the handling of the personal data request of Van der Linde was in breach of its obligations derived from arts. 31(1), 31(6), 36 and 40(1) ER which constituted a direct violation of his rights enshrined in arts. 8, 41 and 47 EU Charter and arts. 36 and 37 ER. Thus, Europol seriously breached obligations conferring rights on Van der Linde directly resulting in the damage suffered by Van der Linde. Based on the foregoing, Van der Linde therefore respectfully requests your Court to:

I. Determine that Europol is liable under art. 268 jo. art. 340 TFEU and arts. 49(3) and 50(1) Europol Regulation for the damage it caused to Van der Linde by breaching its obligations under the Europol Regulation and EU Charter conferring rights on Van der Linde as enshrined in arts. 7, 8, 41 and 47 EU Charter and arts. 36 and 37 Europol Regulation;

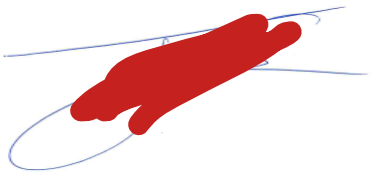
II. Order Europol to compensate the damage suffered by Van der Linde as a direct consequence of the unlawful conduct of Europol in whole, being €50.000 in non-material damage and €26.250 in material damage, as of 9 October 2025, to be increased with the interest due on the date of payment, as set out above, or in part as to be determined by your Court;

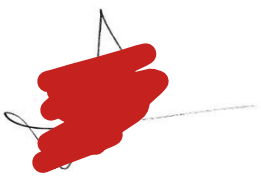
III. Determine that Europol is liable for all as yet unknown damage caused to Van der Linde as a result of the unlawful conduct of Europol;

IV. Order Europol to pay the costs incurred by Van der Linde for the current proceedings to be paid with interest;

V. All to be paid within two weeks after rendering judgment and increased by interests for each day the payment is delayed.

Amsterdam, 9 October 2025





Thomas van der Sommen

Emiel Jurjens

SCHEDULE OF ANNEXES

ANNEX NO	DESCRIPTION OF ANNEX	FIRST AND LAST PAGE OF ANNEX	MENTIONED FOR THE FIRST TIME IN §
A.1	Letter Van der Linde to Europol re. notice of liability, 10 June 2025	1-4	§ 4
A.2	Decision EDPS, 8 September 2022	5-31	§ 8
A.3	Letter Mayor of Amsterdam to Van der Linde re. unlawfulness inclusion deradicalisation program, 25 May 2023	32-34	§ 13
A.4	News article B. Soetenhorst, 'Lastpak Frank van der Linde belandde in de aanpak radicalisering: 'Heb me extreem eenzaam gevoeld', *Het Parool*, 29 April 2023	35-44	§ 13
A.5	News article B. Soetenhorst, 'Interview Hoe de politie zich ontdeed van een dissidente agent', *Het Parool,* 23 September 2023	45-48	§ 14
A.6	Decision Ministry of Justice and Safety, re. rectification NCTV, 7 September 2023	49-52	§ 17
A.7	Judgment District Court of Amsterdam 3 November 2023, AMS 22/1390	53-61	§ 17
A.8	Letter Minister of Justice and Safety to Van der Linde, 30 June 2025	62-67	§ 18
A.9	Decision Dutch Data Protection Authority, 12 March 2025	68-75	§ 19
A.10	Letter Van der Linde to Police re. data access request, 3 September 2019	76-77	§ 21
A.11	Decision Police (annulled), 17 October 2019	78-81	§ 21

A.12	Decision Police (new), 21 October 2022	82-88	§ 23
A.13	Judgment District Court of Amsterdam 8 April 2021, AMS 19/2518	89-93	§ 26
A.14	Interim judgment District Court of Amsterdam 13 April 2022, AMS 19/6327	94-100	§ 27
A.15	Letter District Court of Amsterdam re. forensic expert, 16 April 2024 AMS 19/6327	101-108	§ 29
A.16	Letter Van der Linde to Police re. rectification request, 15 November 2022	109-110	§ 32
A.17	Decision Police (annulled) re. rectification SIENA messages, 31 January 2023	111-116	§ 32
A.18	Decision Police re. complaint, 11 April 2023	117-118	§ 32
A.19	Judgment District Court of Amsterdam 12 March 2025, AMS 23/990	119-123	§ 33
A.20	E-mail Police to Van der Linde re. intended appeal, 26 March 2025	124-128	§ 33
A.21	Decision Police (new), 29 September 2025	129-135	§ 34
A.22	E-mail Police to Van der Linde re. the SIENA system, 9 November 2023	136-140	§ 40
A.23	E-mails Europol to Van der Linde, 13 February, 27 March and 25 May 2025	141-147	§ 40
A.24	Letter Van der Linde to Europol re. data access request, 11 February 2020	148-149	§ 41

A.25	Decision Europol refusing data access, 11 June 2020	150-151	§ 41
A.26	Complaint Van der Linde against Europol, 6 October 2020	152-154	§ 42
A.27	Letter Europol to Van der Linde, 3 February 2025	155-157	§ 67
A.28	E-mail EDPS to Van der Linde, 21 October 2022	158-161	§ 68
A.29	Decision review EDPS, 30 January 2023	162-165	§ 69
A.30	Complaint Van der Linde against Europol, 3 February 2025	166-175	§ 70
A.31	Letter District Court of Amsterdam re. investigation forensic expert, 3 June 2025	176-183	§ 72
A.32	E-mail Van der Linde re. trauma and panic attacks, 7 March 2022	184-188	§ 220
A.33	E-mail Van der Linde to GP Van der Cingel, 7 April 2025	189-191	§ 220
A.34	Letter GP Van der Cingel, 10 December 2021	192-193	§ 220
A.35	E-mail Van der Linde to former lawyer re. serious risk of Europol terrorism association, 4 February 2022	194-195	§ 222
A.36	E-mail Van der Linde to Mayor of Amsterdam and Municipal Secretary re. travel issues, 6 February 2025	196-197	§ 222