ChatGPT

GDPR & AI Cases and Guidance Dataset

Below is a JSON-formatted dataset of authoritative GDPR cases and guidance related to AI systems (LLMs, chatbots, etc.), followed by a **signal taxonomy** defining the violation signals used.


```
{
  "dataset": [
    {
      "id": "gs_001",
      "title": "WP29/EDPB Guidelines on Automated Decision-Making and
Profiling",
      "authority": "Article 29 Working Party (endorsed by EDPB)",
      "jurisdiction": "EU",
      "date": "2018-02-06",
      "source_url": "https://ec.europa.eu/newsroom/article29/redirection/
document/49826",
      "excerpt":
"Profiling may identify special categories of data by inference (for example
inferring an individual's state of health from records of their food shopping).
The controller must also satisfy the conditions in Article 9(2) for special
categories of data inferred from profiling [1].",
      "ai_relevance_tags": ["profiling", "automated_decision",
"special_category", "transparency"],
      "facts_summary": [
        "Comprehensive guidelines explaining GDPR's provisions on profiling and
solely automated decisions.",
        "Clarifies that inferring sensitive traits (health, political opinions,
etc.) through profiling creates **special category data** which triggers GDPR
Article 9 requirements [1].",
        "Emphasizes **transparency** – individuals must be informed about
profiling and its purposes, and explicitly told of their right to object [2]
[3].",
        "Requires a **lawful basis** for any profiling (consent, legitimate
interest with balancing, etc.) [3], and if results are used for automated
decisions, often **explicit consent** or other Art 22 exceptions are needed
[4].",
        "Stipulates controllers must implement safeguards: meaningful
information about logic involved, human intervention for high-impact automated
decisions, regular algorithmic fairness and accuracy testing [5] [6]."
      ],
      "questions": [
        "Does the system infer or create any special category personal data
(e.g. inferring health status or political views) from user input or profiles?",
```

```
"If the AI system profiles individuals or makes automated decisions, has the organization provided meaningful information about the logic involved and ensured individuals can exercise their rights (e.g. to object or seek human review)?",
        "Has a lawful basis been identified for all profiling and automated decision-making activities, and if special category data is involved, is there a valid Article 9(2) condition (such as explicit consent)?",
        "Has the organization implemented measures to ensure profiling is fair, non-discriminatory, and accurate (e.g. algorithmic audits and bias testing)?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_CONDITION_FOR_SENSITIVE", "SPECIAL_CATEGORY_INFERENCE", "NO_LAWFUL_BASIS"],
          "gdpr_refs": ["9(1)", "9(2)", "5(1)(a)"],
          "rationale": [
            "Guidance confirms that inferring sensitive data (like health or politics) counts as processing special category data, requiring a GDPR Art 9(2) condition [1]. The system's creation of such data without meeting an exception would violate Art 9.",
            "If no valid lawful basis was established for this sensitive data profiling, it fails Art 6 and Art 5(1)(a) (lawfulness). The guidelines stress all personal data processing must rest on a valid basis [7]."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY", "NO_MEANINGFUL_EXPLANATION", "NO_DSR_OBJECTION"],
          "gdpr_refs": ["5(1)(a)", "13", "14", "15", "21", "22"],
          "rationale": [
            "The guidelines require informing individuals about profiling logic and their rights [2]. Not providing this information (e.g., no meaningful explanation of AI decisions) breaches transparency obligations (Arts 13–14) and data subject rights (Arts 15, 21, 22).",
            "Art 5(1)(a) fairness/transparency is violated if users aren't clearly told they're subject to profiling or automated decisions, or if they cannot seek human intervention [5]."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS", "INVALID_CONSENT"],
          "gdpr_refs": ["6(1)", "7", "22(2)(c)"],
          "rationale": [
            "Controllers must choose an appropriate lawful basis that matches
```

```
the context of profiling [8] [9]. If none was documented, that's a violation of Art 6(1).",

"If relying on consent for profiling or automated decisions, it must be explicit and meet GDPR standards [10]. The guidelines note explicit consent is generally required for significant automated decisions [4] – failing to obtain this would violate Art 7 and Art 22(2)(c)."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["BIAS_OR_INACCURACY",
"NO_ALGORITHM_AUDIT"],
          "gdpr_refs": ["5(1)(d)", "5(1)(a)"],
          "rationale": [
            "The guidelines urge controllers to test and prevent errors or bias in profiling algorithms [6]. If the system has not been audited for fairness or accuracy, there is a risk of violating Art 5(1)(d) (accuracy) and Art 5(1)(a) (fairness).",

"Without evidence of measures to detect and correct bias, compliance cannot be confirmed. It **needs review** to ensure algorithmic outputs do not unjustifiably disadvantage certain groups [11]."
          ]
        }
      ],
      "ambiguity_notes": "There is some debate about the exact scope of the "right to an explanation." While these guidelines emphasize providing meaningful information about automated decision logic, GDPR does not explicitly guarantee a full explanation. Interpretation of how much detail must be provided can vary. Additionally, determining when profiling creates special-category data by inference can be complex – it depends on context and the nature of data, which may require case-by-case analysis."
    },
    {
      "id": "gs_002",
      "title": "EDPB ChatGPT Task Force Report – Interim Issues List",
      "authority": "EDPB",
      "jurisdiction": "EU",
      "date": "2024-05-23",
      "source_url": "https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf",
      "excerpt": "When web scraping personal data from publicly accessible sources such as websites, the requirements of Article 14 GDPR apply... The exemption of Article 14(5)(b) could apply only if all requirements are fully met [12]. By contrast, when personal data is collected directly from users interacting with ChatGPT, Article 13 applies – it's particularly important to inform users that their input may be used for training [13]. The principle of data
```

```
accuracy must be complied with; ChatGPT’s probabilistic outputs may be biased or made-up, yet end users could take them as factual – thus controllers must address accuracy [14] [15].",
      "ai_relevance_tags": ["LLM", "model_training", "web_scraping", "transparency", "accuracy", "DSR_access", "children"],
      "facts_summary": [
        "EDPB’s ChatGPT Task Force identified key GDPR compliance issues across EU investigations into OpenAI’s ChatGPT service [16] [17].",
        "Highlighted **transparency** duties: if personal data is scraped from the web for training, Article 14 notices to individuals are required unless a narrow Art 14(5)(b) exception applies [12]. Users directly providing data to the chatbot must get clear Article 13 information, including that their prompts may be reused for training [13].",
        "Noted **lawful basis** concerns: OpenAI must identify a valid legal basis for both training on scraped data and processing user inputs. Many SAs questioned if “legitimate interests” can justify extensive training processing [18] [19].",
        "Emphasized the **accuracy principle** (Art 5(1)(d)): ChatGPT can produce incorrect or fabricated personal information. Controllers still must take steps to prevent and rectify inaccuracies about individuals [15].",

"Raised **fairness and safeguards**: Users may input personal data (even minors’ data) despite terms prohibiting it. The service should not transfer the burden to users – instead it must implement measures (age checks, filters) to prevent unfair outcomes [20] [21].",
        "Addressed **data subject rights**: OpenAI needs easy, accessible mechanisms for users (and non-users) to request erasure or correction of personal data in training sets or outputs. A notable challenge is **rectification** – if the model output about someone is wrong, it may be technically infeasible to correct the model without retraining, so offering erasure is crucial [17] [22].",
        "Stressed **data protection by design**: The report urges incorporating privacy safeguards from development through deployment, e.g. minimizing data collection, allowing opt-outs, and ensuring compliance is built into model design [23]."
      ],
      "questions": [

"If the AI model was trained on scraped personal data from the internet, did the organization either provide Article 14 notices to those individuals or properly document why an Article 14(5)(b) exception (disproportionate effort) applies?",
        "Are users (and potentially non-users) clearly informed that any personal data they input into the chatbot might be retained and used for model training purposes (Article 13 transparency)?",
        "What lawful basis has been determined for processing personal data during model training and interactions? If relying on legitimate interests, has a rigorous necessity and balancing test been documented given the breadth of data used?",
```

```
        "How does the organization ensure the outputs generated about
individuals are accurate and up-to-date, and how can individuals correct or
remove false personal information produced by the AI (given the model's tendency
to hallucinate)?",
        "Has the organization implemented measures to prevent the model from
processing personal data of minors or special category data without proper
safeguards (e.g. age verification, filters for sensitive content)?",
        "Can data subjects request deletion of their data from the training set
or model, and how is such a request honored in practice (for example, by
deleting associated embeddings or retraining)?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_ART14_NOTICE",
"LACK_TRANSPARENCY"],
          "gdpr_refs": ["14", "5(1)(a)"],
          "rationale": [
            "The service used web-scraped personal data without providing
Article 14 notices [12] and likely did not meet the strict criteria of Art 14(5)
(b) (which is narrowly construed). This is a transparency failure.",
            "Each individual whose data was scraped should have been informed
within one month. Not doing so violates Art 14 and the transparency principle
(Art 5(1)(a))."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
          "gdpr_refs": ["13", "5(1)(a)"],
          "rationale": [
            "Until intervention, users were not explicitly informed at sign-up
that their prompts could be used to further train the model [13]. This omission
breaches Art 13 requirements to inform data subjects of processing purposes.",
            "Transparency is a core principle; failing to disclose training use
of user-provided data is unfair and non-transparent (Art 5(1)(a))."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["NO_LAWFUL_BASIS",
"INVALID_LEGITIMATE_INTEREST"],
          "gdpr_refs": ["6(1)", "5(1)(a)"],
          "rationale": [
            "It's unclear on what legal basis personal data was processed for
training. If the controller claims **legitimate interest**, it must demonstrate
that interest and that it outweighs individuals' privacy rights [18]. Given the
vast scope of data, this is debatable and **needs further review**.",
```

```
            "Without a clearly documented lawful basis for each processing
purpose (training vs operation), the processing may violate Art 6(1). The
fairness principle (Art 5(1)(a)) is also at stake if data subjects had no say or
awareness."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["INACCURATE_OUTPUT",
"NO_DATA_ACCURACY_MEASURES"],
          "gdpr_refs": ["5(1)(d)", "16"],
          "rationale": [
            "The AI sometimes generated incorrect or fabricated personal
information about people [15]. If no effective measures exist to prevent or
correct such inaccuracies, it violates the data accuracy principle (Art 5(1)
(d)).",
            "Data subjects have the right to rectification (Art 16). Since
rectifying a model's output is not straightforward, the lack of a mechanism to
address known false outputs means the controller is not upholding accuracy
obligations."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["CHILDREN_NOT_PROTECTED",
"NO_PRIVACY_BY_DESIGN"],
          "gdpr_refs": ["5(1)(a)", "25(1)"],
          "rationale": [
            "The service had no robust age-gating or verification initially [24],
meaning minors could access it despite handling personal data and potentially
seeing inappropriate content. This contravenes fairness (processing children's
data without safeguards is unfair) and potentially legal requirements for
parental consent (if any data falls under child consent age).",

"Not implementing age verification or content filters from the start is a
failure of data protection by design/default (Art 25(1)), as the system did not
incorporate protective measures for vulnerable groups."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["17", "21"],
          "rationale": [
            "The platform established a procedure for data subjects to request
deletion of personal data and has been honoring those requests (e.g. via a web
form for removal from training data). If deletion requests are processed and
training data can be removed, it complies with Art 17.",
```

```
            "No evidence suggests that erasure or objection requests are being refused. Assuming the controller provides a way to opt-out of future processing (stop using one’s data), this aspect would be compliant."
          ]
        }
      ],
      "ambiguity_notes": "There is ongoing debate on how to practically implement rights like rectification and erasure in AI models. The Task Force notes OpenAI’s approach of offering erasure when rectification of a trained model is infeasible [25] [22]. It remains ambiguous how thoroughly training data can be purged from an LLM and whether such erasure fully prevents the model from generating that data. Also, reliance on legitimate interests for AI training is contentious; regulators differ on whether it’s appropriate, which creates uncertainty for controllers choosing a lawful basis."
    },
    {
      "id": "gs_003",
      "title": "Garante (Italy) vs. OpenAI – ChatGPT Temporary Ban and Requirements",
      "authority": "Garante (Italian DPA)",
      "jurisdiction": "Italy",
      "date": "2023-03-31 (provisional order), 2023-04-11 (requirements), 2023-04-28 (service reinstated)",
      "source_url": "https://www.gpdp.it/newsroom/archivio/comunicati-stampa/2023",
      "excerpt": "The Italian SA found that OpenAI had **no legal basis** for the mass collection and processing of personal data to train ChatGPT’s algorithms – data was scraped from the web and processed in ways incompatible with users’ expectations. Additionally, the service provided **no notice to data subjects** whose data were used for training, and lacked any age-verification mechanism to protect minors. The Garante imposed a temporary ban and ordered OpenAI to quickly implement measures: an easily accessible privacy notice, age gating, a mechanism for users and non-users to request **erasure** of their data, and an opt-out from processing [26] [27].",
      "ai_relevance_tags": ["LLM", "model_training", "web_scraping", "lawful_basis", "transparency", "DSR_erasure", "children"],
      "facts_summary": [
        "On March 31, 2023, Italy’s DPA issued an emergency order halting ChatGPT over GDPR concerns [27]. Key issues: *unlawful* data collection from the internet, lack of transparency, and absence of age controls for minors.",
        "OpenAI had scraped personal data (from public websites, social media, etc.) to train the GPT model without informing individuals or obtaining any legal basis (no consent, contract, etc.). The Garante viewed this as **unlawful processing** under Articles 5 & 6 [27].",
        "Users had not been given any privacy notice about how their conversations or others’ data might be used. The service launched without an Article 13/14-compliant notice, violating transparency obligations.",
        "ChatGPT had no age verification, yet was accessible to young users.
```

```
This raised child data protection issues, as content might not be appropriate
and parental consent was not obtained for under-14s (the applicable age in
Italy).",

"The DPA gave OpenAI a **to-do list** to lift the ban: implement a clear privacy
notice in Italian, put up an age-gate (initially self-declaration plus a plan
for stronger verification), provide user-friendly ways to exercise data subject
rights (especially erasure/correction of personal data), and allow an opt-out to
exclude one's data from training.",
        "OpenAI complied by the deadline (April 30, 2023): it published an
improved privacy policy, added an age check, created a form for EU individuals
to request deletion of personal data, and offered a way to object to use of data
for training. The service was reinstated in Italy on April 28, 2023 [28] [29] ."
      ],
      "questions": [
        "Did the organization establish a valid lawful basis (e.g. consent or
legitimate interests with necessity test) for collecting and using personal data
from the internet to train the AI model?",
        "Before processing people's data for training or responding, were data
subjects provided with an adequate privacy notice (per Articles 13 or 14)
informing them of this use?",
        "What measures are in place to prevent underage individuals from using
the AI service, and are those measures effective (e.g. robust age
verification)?",
        "Does the service offer individuals (both users and non-users) a way to
request deletion of their personal data from the model's training dataset or
outputs, and are such requests honored promptly?",

"Can individuals opt out from having their personal data used to further train
or improve the AI model (and if so, how is this opt-out implemented)?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS"],
          "gdpr_refs": ["6(1)", "5(1)(a)"],
          "rationale": [
            "OpenAI admitted it had not clearly identified a legal basis for
using vast personal data from the web. The Garante found no consent or other
valid basis was in place [30] . This is a direct Art 6 violation.",
            "Processing personal data at such scale without a lawful basis also
breaches the principle of lawfulness/fairness (Art 5(1)(a)). The Italian DPA
highlighted this as a fundamental issue."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
```

```
          "gdpr_refs": ["13", "14", "5(1)(a)"],
          "rationale": [
            "No privacy notice was given to data subjects at all initially. Web-
scraped individuals weren't informed (Art 14), and even users providing prompts
weren't adequately informed (Art 13). This was explicitly cited by the Garante
[27]
.",
            "This lack of transparency violates Articles 13/14 and the openness
requirement in Art 5(1)(a). The enforcement required OpenAI to post a clear
privacy policy and disclosure as a condition to resume service [28] ."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["CHILDREN_NOT_PROTECTED"],
          "gdpr_refs": ["5(1)(a)", "8", "25(1)"],
          "rationale": [
            "The service had **no age verification** despite being open to
minors [31] . This means potentially unlawful processing of children's data without
parental consent (required by Art 8 in many cases).",
            "Allowing minors onto an AI that can produce harmful content,
without safeguards, was considered unfair and against data protection by design
(Art 25). The DPA specifically flagged absence of age-gating as a violation [32] ."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["17", "21"],
          "rationale": [
            "In response to the order, OpenAI implemented a form for anyone to
request **erasure** of personal data, fulfilling Art 17. If a user or non-user
submits a deletion request, OpenAI now will remove that data from training where
feasible.",
            "The Garante's requirements included enabling objections to
processing. OpenAI added an opt-out for training use of conversations, giving
data subjects an Art 21 mechanism. With these measures in place, the compliance
on DSRs (erasure/objection) can be considered satisfactory (hence a pass)."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["6(1)(f)", "21"],
          "rationale": [

"After the intervention, OpenAI asserted **legitimate interests** as its lawful
basis in its updated privacy notice. While this basis is debatable, OpenAI did
conduct a Legitimate Interests Assessment and added opt-out rights for users
```

```
[18].",
            "Given that the service was allowed to resume and the DPA did not
further contest the new basis at that time, we treat it as provisionally
acceptable. The presence of an opt-out means data subjects can exercise their
Art 21 right to object, mitigating the impact of using legitimate interests."
          ]
        }
      ],
      "ambiguity_notes": "This case left open the question of what legal basis
is appropriate for training large AI models on public data. OpenAI moved to
legitimate interests, but regulators haven't definitively agreed this is lawful
– it's a grey area whether broad AI training can count as a legitimate interest.
Additionally, how effectively an individual's data can be removed from an
already-trained model remains technically uncertain; the solution (offer
erasure) was a pragmatic compliance step, but the model may still retain some
influence from that data, raising questions about completeness of erasure."
    },
    {
      "id": "gs_004",
      "title": "CNIL (France) – Enforcement against Clearview AI (Facial
Recognition Database)",
      "authority": "CNIL (France) – Restricted Committee Sanction",
      "jurisdiction": "France/EU",
      "date": "2022-10-20 (final decision)",
      "source_url": "https://www.cnil.fr/en/facial-recognition-20-million-euros-
penalty-against-clearview-ai",
      "excerpt": "Key Findings: *Unlawful processing of personal data* (breach
of Article 6)… *Individuals' rights not respected* (Articles 12, 15, 17)… *Lack
of cooperation* with the CNIL (Article 31)[33][34]. The CNIL fined Clearview AI
€20 million and ordered it to stop collecting and processing the facial images
of individuals in France without a legal basis, and to delete existing data
within 2 months[35].",
      "ai_relevance_tags": ["facial_recognition", "model_training",
"biometrics", "lawful_basis", "DSR_access", "DSR_erasure", "cross_border"],
      "facts_summary": [

"Clearview AI amassed a database of 3+ billion facial images by scraping photos
from websites and social media without consent. It offered a facial recognition
service allowing identification of individuals from a photo.",

"After complaints, CNIL investigated. In October 2022, CNIL's Restricted
Committee found multiple GDPR violations[33]:",
        "- **No lawful basis**: Clearview had no valid legal basis for its
processing (it claimed legitimate interest in combating crime, but this was not
applicable for its broad commercial use). Article 6 was violated[36].",
        "- **Unlawful processing of sensitive data**: Face images are biometric
data (special category) used for unique ID. Clearview did not meet any Art 9(2)
condition (no explicit consent, etc.), making the processing **illegal**.",
```

```
        "- **Failure to inform data subjects**: No Article 14 notice was given
to the millions of people scraped. People generally had no idea Clearview
collected their images, breaching transparency obligations.",

"- **Rights infringements**: Clearview ignored individuals' requests (or made it
overly difficult to exercise rights). CNIL noted violations of the rights of
access and erasure (Arts 15 and 17) [36] - e.g., individuals could not get their
data or get it deleted effectively.",
        "- **Lack of cooperation**: Clearview also did not respond to CNIL's
formal orders (violating Art 31 duty to cooperate) [33].",
        "Sanctions: €20 million fine (maximum under GDPR), an order to **stop
processing** faces of people on French territory and to **delete** existing
French individuals' data within 2 months [34]. Additionally, a daily penalty for
non-compliance was set to pressure deletion.",
        "Clearview, a US company with no EU office at the time, was also cited
for not having an EU representative (Art 27) in earlier CNIL communications (and
similarly fined by other EU DPAs)."
      ],
      "questions": [
        "Is personal data (images) being collected from the internet without
informing individuals, and if so, what is the legal basis for this collection
and use?",
        "If the AI system processes biometric data (like facial images for
identification), has the company obtained explicit consent or met another
Article 9(2) exception for special category data?",
        "Does the organization provide an accessible mechanism for individuals
to exercise their rights (access, deletion) regarding their data in the AI's
database or model?",
        "How does the company ensure compliance with data subject access and
erasure requests, especially given the large-scale or automated nature of the
data collection?",

"Has an EU representative been appointed for GDPR compliance, given that the
company has no EU establishment but targets EU residents?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS",
"UNLAWFUL_SENSITIVE_PROCESSING"],
          "gdpr_refs": ["6(1)", "9(1)"],
          "rationale": [
            "Clearview scraped and used images without consent or any valid
legal basis. CNIL explicitly found a breach of Art 6 - no lawful basis [36]. This
is a fundamental failure.",
            "Because the data is biometric (faceprints), an Art 9(2) condition
was needed but none applied. Thus, processing sensitive data was unlawful per
Art 9(1)."
```

```
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY",
"NO_ART14_NOTICE"],
          "gdpr_refs": ["14", "12"],
          "rationale": [
            "Individuals were never informed that their photos were collected.
This violates Art 14's obligation to inform data subjects when data is obtained
indirectly. CNIL flagged the complete lack of notice.",
            "The overall transparency and communication duties (Art 12) were
breached – Clearview's users (police clients) knew about the service, but the
people in the photos did not."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["DSR_IGNORED"],
          "gdpr_refs": ["15", "17", "12(2)"],
          "rationale": [
            "The company did not properly respond to access or deletion
requests. CNIL noted Clearview failed to honor Art 15 and 17 rights [36].",
            "Under Art 12(2), controllers must facilitate the exercise of
rights. Clearview's unresponsiveness or cumbersome process (like requiring
excessive proof) meant data subjects' rights were effectively denied."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NON_COOPERATION",
"NO_ART27_REPRESENTATIVE"],
          "gdpr_refs": ["31", "27"],
          "rationale": [
            "Clearview ignored CNIL's formal notice and did not fully cooperate
with the investigation (violating Art 31) [33]. Lack of cooperation is itself a
GDPR infringement noted in the decision.",
            "The company had no EU representative despite targeting EU
residents, breaching Art 27. This was observed by EU authorities (Italy's DPA
also ordered designation of a rep [37] [38])."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(e)", "32"],
          "rationale": [
            "Clearview instituted an EU-opt-out webform and claims to have
```

```
ceased storing data of EU residents after the sanctions. If it indeed stopped retention of EU personal data and purged existing data, it would align with storage limitation (Art 5(1)(e))."],
            "Security measures weren't a focal point of CNIL's decision beyond data deletion. Assuming Clearview secures any remaining data properly, there's no evidence of a security violation now."
          ]
        }
      ],
      "ambiguity_notes": "This case underlines jurisdictional challenges: Clearview had no EU presence and initially ignored EU orders. Enforcing deletion and fines across borders is difficult – Clearview has appealed or not paid in some jurisdictions. It raises questions about effectiveness of GDPR remedies against a non-cooperative foreign entity. Also, the definition of biometric data came into play – any facial image used for identification was treated as special category data, though Clearview argued it was just publicly available data. Regulators clearly took the stance that faces = biometric identification, hence sensitive, but companies might contest that interpretation."
    },
    {
      "id": "gs_005",
      "title": "Garante (Italy) – Clearview AI Sanction (Web Scraping of Biometric Data)",
      "authority": "Garante per la Protezione dei Dati Personali (Italy)",
      "jurisdiction": "Italy",
      "date": "2022-02-10 (decision)",
      "source_url": "https://www.gpdp.it/newsroom",
      "excerpt": "The Italian SA found several infringements by Clearview AI Inc. Personal data, including biometric and geolocation information, were processed *unlawfully*, without an appropriate legal basis – the company's claimed legitimate interest does not qualify as such. Additionally, the company violated fundamental principles like *transparency*, *purpose limitation*, and *storage limitation*; it failed to provide the information required by Articles 13–14, failed to respond to an access request (Article 15) in time, and had not appointed an EU representative [39]. The Garante fined Clearview €20 million, banned further data scraping and processing of Italians' data, ordered all data (including biometrics) erased, and required an EU representative to be designated [40] [41].",
      "ai_relevance_tags": ["facial_recognition", "biometrics", "web_scraping", "lawful_basis", "transparency", "purpose_limitation", "data_retention", "DSR_access"],
      "facts_summary": [
        "In March 2022, Italy's DPA reached a similar conclusion as France regarding Clearview's activities. Key findings from the Italian decision [39]:",
        "– **Illegal processing & no legal basis**: Clearview's scraping and using of Italians' images (faces) had no valid lawful basis. The company's argument of legitimate interest was rejected as insufficient for this scope [42].",
```

```
        "- **Transparency failures**: No privacy notice was given (Arts 13/14), so people had no idea their photos were collected [43].",
        "- **Purpose and storage limitations violated**: The data was collected for broad, undefined purposes (law enforcement, etc.) not explicit to data subjects, and kept indefinitely – violating purpose limitation and storage limitation principles [44].",
        "- **Data subject rights ignored**: Clearview didn't properly handle at least one Italian's access request (Article 15) – not replying in time [45].",

"- **No EU representative**: Clearview hadn't appointed a representative in the EU as required by Art 27, despite operating across EU markets [37].",
        "Sanctions mirrored France: €20 million fine; an **order to stop** any further scraping or use of Italians' images; an **order to delete** all existing Italian personal data (including biometric templates) from its systems [41]; and an order to designate an EU representative [46] [47]."
      ],
      "questions": [
        "Did the company rely on 'legitimate interest' to justify scraping and processing of personal images for facial recognition, and has that been deemed inappropriate by regulators?",
        "Has the company clearly defined and limited the purpose for which it collects personal images, and does it avoid using them in new, incompatible ways (purpose limitation)?",
        "Are there data retention policies ensuring biometric and personal data are not stored longer than necessary, or is data kept indefinitely without justification?",
        "Did the organization fail to respond to any data subject access requests within the GDPR timeframe, indicating a broader issue with handling individuals' rights?",
        "If the company operates without an EU establishment while offering services involving EU individuals' data, has it appointed an EU representative as required?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["INVALID_LI_BASIS", "UNLAWFUL_SENSITIVE_PROCESSING"],
          "gdpr_refs": ["6(1)(f)", "9(1)"],
          "rationale": [
            "The Italian Garante explicitly rejected Clearview's claim that its **legitimate interest** justified this processing [42]. Using LI for mass biometric data scraping was deemed invalid, hence no lawful Art 6 basis.",
            "Processing biometric data (faces) without consent or another Art 9 exception means an Art 9(1) violation. The decision highlighted the unlawful nature of processing special categories with no exemption."
          ]
        },
```

```
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["PURPOSE_CREEP",
"EXCESSIVE_RETENTION"],
          "gdpr_refs": ["5(1)(b)", "5(1)(e)"],
          "rationale": [
            "Clearview collected data for broad purposes (it wasn't clear or
communicated) and then used it in various contexts. This violates the **purpose
limitation** principle (Art 5(1)(b)) [43] .",
            "Data was stored indefinitely. Keeping personal data without time
limits or review breaches the **storage limitation** principle (Art 5(1)(e)).
The Garante found lack of any retention policy problematic."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["DPO_&_REPRESENTATIVE_ISSUES"],
          "gdpr_refs": ["27", "37"],
          "rationale": [
            "No EU representative was appointed, flouting Article 27 obligations
[37] . A company serving EU markets must designate one – Clearview did not, as
noted by both Italian and French authorities.",
            "While not explicitly about a DPO, the overall compliance failures
suggest governance issues. (In the decision, Art 27 was clearly breached; Art 37
DPO requirement might apply given large-scale sensitive data – unclear if they
had one, but representative was definitely missing.)"
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["15", "12(3)"],
          "rationale": [
            "Post-investigation, Clearview claimed it set up a process for
individuals (including Italians) to access their data. If it now responds to
Art 15 requests within one month and provides the data, that aspect could be
compliant.",
            "Assuming Clearview now has a proper rights portal or email for EU
individuals and it actually complies, then it would not be failing the access
right currently (hence a pass on this specific question)."
          ]
        }
      ],
      "ambiguity_notes": "The fine and orders in Italy were similar to those in
France, reinforcing a consistent EU stance. However, Clearview's subsequent
compliance is questionable – reports indicated it geoblocked EU queries rather
than truly deleting data, raising the issue: Is blocking access enough, or must
data actually be erased? DPAs insist on erasure, but enforcing that abroad is
```

```
tricky. This case also illustrates how DPAs interpret ‘legitimate interests’ narrowly for expansive AI data uses – something companies might dispute but haven’t tested in court yet."
    },
    {
      "id": "gs_006",
      "title": "CNIL Guidelines – AI System Development and GDPR Compliance",
      "authority": "CNIL (France)",
      "jurisdiction": "France/EU",
      "date": "2024-06-07",
      "source_url": "https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr",
      "excerpt": "Designers and developers of AI systems often believe the GDPR hinders AI innovation – this is false. They must be aware that training datasets *sometimes include personal data*. Use of such data poses risks to individuals, which must be addressed to develop AI in ways that respect rights and freedoms [48]. **Step 1: Define a purpose** – an AI system using personal data must have a well-defined, explicit, legitimate purpose. This frames and limits what data can be used for training, to avoid storing or processing unnecessary data [49]. The purpose must be determined from the project’s start; unanticipated uses don’t waive this requirement [50].",
      "ai_relevance_tags": ["guidance", "model_training", "purpose_limitation", "data_minimization", "lawful_basis", "DPIA", "data_retention"],
      "facts_summary": [
        "In 2024, CNIL published practical recommendations (8 steps) for integrating GDPR compliance into AI development [51] [52]. Key points include:",
        "1. **Purpose Definition**: Clearly define the specific purpose for using personal data in the AI project from the outset [49]. Even for general-purpose AI, you must articulate legitimate objectives. This ensures compliance with purpose limitation – no collecting data ‘just in case’ or for overly broad ends.",
        "2. **Determine Roles & Responsibilities**: Figure out early who is the data controller vs. processor for each dataset and phase (e.g., AI providers creating a model might be controllers for training data). This affects compliance steps (contracts, etc.).",
        "3. **Lawful Basis for each Processing**: Identify an appropriate legal basis for using personal data in training and evaluation. CNIL specifically addressed using **legitimate interest** for AI training – it can be viable if a balancing test is done and rights are protected, but not for special categories without explicit consent [53].",
        "4. **Check Data Re-use**: If using personal data originally collected for one purpose to train an AI for another purpose, assess compatibility or get new consent [54]. Avoid ‘mission creep’.",
        "5. **Data Minimization**: Use the smallest dataset necessary. Limit features to those relevant. The guide gives strategies like selecting limited attributes or anonymizing where possible [55]. Don’t hoard data “because AI needs big data” – still need justification.",
        "6. **Set Retention Periods**: Establish how long personal data
```

```
(training data, model outputs) will be kept [56]. Don't keep training data
indefinitely once the model is built unless necessary – define criteria (e.g.,
retraining intervals) for deletion [57].",
        "7. **DPIA**: Conduct Data Protection Impact Assessments for high-risk
AI projects (e.g., those involving profiling, sensitive data, or decisions with
legal effects) [58]. The guidance stresses DPIAs as a mandatory step before
deployment.",
        "8. **Document & Justify** (Accountability): Maintain documentation of
the above – purposes, basis, assessments – and implement privacy by design
measures throughout (from dataset creation to model tuning)."
      ],
      "questions": [
        "At the start of the AI project, was a specific and legitimate purpose
defined for processing personal data, and is all personal data usage limited to
that purpose?",
        "Have the roles been determined (who is the data controller for the
training data vs. the AI service, and are there data processing agreements in
place if needed)?",

"What is the legal basis for using personal data in model training – for
example, has the organization documented a legitimate interests assessment or
obtained consent as appropriate?",
        "If personal data collected for one context is being reused to develop
an AI model for another purpose, was compatibility of purpose analyzed or new
consent obtained?",
        "Does the project apply data minimization – using only the data and
attributes necessary for the training objective – and has consideration been
given to anonymization or synthetic data to reduce personal data use?",
        "Has a Data Protection Impact Assessment been conducted to evaluate the
risks of the AI processing (especially if it involves sensitive data or
profiling individuals)?",
        "Are there defined data retention and deletion policies for personal
data used in training (and is model output or learned data periodically reviewed
for continued necessity)?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(b)"],
          "rationale": [
            "The project has a clear statement of purpose (e.g., "predictive
maintenance on user-provided data for service improvement"). All data collected
aligns with this specific purpose. This meets purpose limitation (Art 5(1)
(b))."",
            "No evidence of function creep: they are not repurposing the data
for unrelated objectives. Thus, this aspect is compliant."
          ]
```

```
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["ROLE_CONFUSION"],
          "gdpr_refs": ["24", "28"],
          "rationale": [
            "It's not immediately clear who the controller is for the training
data – the AI vendor or the client using the model. If roles aren't clearly
assigned, responsibility under Art 24 is blurred.",
            "Without proper controller/processor contracts (Art 28) in place,
compliance is uncertain. This needs review to ensure accountability is correctly
allocated."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS"],
          "gdpr_refs": ["6(1)"],
          "rationale": [
            "No documented lawful basis was provided for processing personal
data in training. The team proceeded without performing a legitimate interest
balancing or getting consent, etc.",
            "Under Art 6(1), processing is unlawful without a basis. This
fundamental step was skipped, so it's a clear failure."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(c)"],
          "rationale": [
            "The developers applied minimization: they only used 5 data fields
out of 20 available, and excluded identifiers not needed for the model. This
indicates compliance with Art 5(1)(c).",
            "They also explored synthetic data for part of the training –
showing efforts to reduce real personal data usage. This proactive approach
aligns with GDPR principles."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_DPIA"],
          "gdpr_refs": ["35"],
          "rationale": [
            "The AI system profiles individuals in a way that likely triggers
high risk (automated assessment affecting individuals), but no DPIA was done. If
a DPIA was required and missing, that's a direct violation of Art 35.",
            "CNIL's guidance stresses DPIAs for AI [58]. Not performing one when
```

```
warranted means risks weren’t properly evaluated or mitigated."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["UNDEFINED_RETENTION"],
          "gdpr_refs": ["5(1)(e)"],
          "rationale": [
            "The team has not set a clear retention period for the training
dataset or model outputs. They vaguely intend to keep data “as long as useful.”
That’s not a defined period, raising concerns under Art 5(1)(e).",

"This is flagged for review – a proper deletion schedule or criteria should be
established (e.g., delete raw data after model validation, retrain model every X
years and purge old data). Until that’s resolved, compliance is questionable."
          ]
        }
      ],
      "ambiguity_notes": "Applying GDPR principles in AI development can be
tricky. For instance, determining when personal data is truly necessary (data
minimization) might be debated among developers. CNIL’s stance is conservative:
if in doubt, leave it out or anonymize. Also, relying on legitimate interest for
training data is mentioned by CNIL, but still somewhat gray – it requires solid
justification and some regulators (or the upcoming AI Act) might push for
consent in certain AI contexts. The guidance tries to give clarity, but
controllers still face ambiguity in assessing compatibility of secondary data
use and how to effectively anonymize data for AI (since truly anonymizing high-
dimensional data can be challenging)."
    },
    {
      "id": "gs_007",
      "title": "ICO (UK) Guidance – AI and Data Protection (Auditing
Framework)",
      "authority": "Information Commissioner’s Office (UK)",
      "jurisdiction": "UK (UK GDPR)",
      "date": "2020-07-30 (initial publication), updated 2021–2023",
      "source_url": "https://ico.org.uk/for-organisations/guide-to-data-
protection/key-data-protection-themes/guidance-on-ai-and-data-protection/",
      "excerpt":
"The ICO’s guidance outlines best practices and interpretations for **data
protection-compliant AI**. It emphasizes accountability: organizations should
document and justify each decision to use AI with personal data, and be able to
demonstrate compliance (eg. via DPIAs, risk assessments) 59 60 . Key areas
include **transparency** – informing individuals about AI processing in clear
terms, including the purposes, data sources, and outputs affecting them 61 62 .
**Lawfulness** – you must have an appropriate lawful basis for each stage (eg.
one for training, another for deployment) and *you cannot swap bases later
without reason* 63 . **Fairness** – avoid bias and discrimination; test your
```

```
models and include human review especially for impactful decisions. **Accuracy** – ensure personal data and AI predictions are accurate and up to date, especially if used in decisions about individuals [64]. **Minimisation & Security** – only use data you actually need and secure it (eg. techniques like encryption, access controls, and even privacy-enhancing technologies for AI) [65] [66].",
      "ai_relevance_tags": ["guidance", "accountability", "transparency", "lawful_basis", "fairness", "accuracy", "data_minimization", "security", "DSR"],
      "facts_summary": [
        "The ICO, in consultation with the Alan Turing Institute, published detailed guidance and an auditing framework for AI systems. It serves as a manual for both organizations and ICO auditors to ensure AI use complies with UK GDPR.",
        "It's structured around GDPR principles applied to AI: **accountability** (governance, risk management), **transparency** and explainability, **lawfulness and fairness**, **purpose limitation**, **data minimisation**, **accuracy**, **security**, and **individual rights** [67] [68].",
        "The guidance recognizes that AI often involves multiple processing stages (data collection, model training, inference). It advises identifying a lawful basis for each stage and purpose [8]. For instance, training might use legitimate interests, while deployment for a user-facing service might be consent or contract – but these must be determined upfront.",
        "It places strong emphasis on **transparency** in AI: organizations should tell people if AI is used in decisions or profiling and provide *meaningful information* about the logic (not the algorithm code, but the criteria and factors) [61] [69]. The ICO references its separate guidance on "Explaining AI decisions" which provides techniques for this.",
        "On **fairness and bias**: The ICO expects organizations to assess AI models for discriminatory outcomes. They should consider the Equality Act and not just GDPR – but from a GDPR view, processing that leads to unjustified bias could be unfair (Art 5(1)(a)). Regular monitoring and bias mitigation strategies are advised.",
        "The guidance also highlights **data minimization** in AI: avoid using personal data if you can achieve the goal with anonymized or synthetic data. Don't just grab entire datasets if only certain features are needed. If possible, use aggregation or perturbation to reduce identification risk [65].",
        "**Security**: due to the complexity of AI systems, ensure robust security at all levels (training data, models, outputs). That includes standard measures (encryption, access logs) and AI-specific concerns (like adversarial example defense, or preventing models from unintentionally leaking training data).",
        "Finally, on **individuals' rights**: AI systems should be designed to accommodate data subject rights. E.g., can you fulfill a subject access request by extracting an individual's data from training records or explaining their profile? The guidance notes the challenges but insists on mechanisms to honor rights like access, rectification, objection (especially to profiling/Automated decision-making under Art 22) [70] [71]."
      ],
```

```
      "questions": [
        "Has the organization documented its decision-making process for
implementing AI, including DPIAs and internal risk assessments, to demonstrate
accountability?",

"Are individuals informed that their personal data will be used in an AI system,
and do they receive an explanation (in general terms) of how the AI affects them
(e.g., in making decisions or profiling)?",
        "Did the organization determine and document a lawful basis for each
phase of the AI's processing of personal data (for example, one for initial
training data processing and another for live deployment), and is that basis
communicated in the privacy notice?",
        "What steps are taken to ensure the AI's outputs or decisions are fair
and not unlawfully biased? Is there human oversight for important decisions and
have the models been tested for bias or discrimination?",
        "Is only the minimum necessary personal data being used to train and
operate the AI? Has consideration been given to using anonymized or less
sensitive data where possible?",
        "What security measures protect personal data in the AI system (during
training and inference), and have measures like encryption, access control, and
robustness against data leakage been implemented?",
        "Can individuals exercise their GDPR rights in relation to the AI's
processing (e.g., access their data, correct or delete it, or opt out of
automated decisions), and are there processes to handle such requests?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(2)", "24", "35"],
          "rationale": [
            "The organization conducted a thorough DPIA before deploying the AI
and has a risk management file. They've kept records of how data is used and
decisions made (accountability fulfilled under Art 5(2) and 24).",
            "When asked, they can produce documentation showing compliance
measures (e.g., meeting minutes evaluating bias mitigation, security design
docs). This indicates strong accountability."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
          "gdpr_refs": ["13", "15"],
          "rationale": [
            "Users are not informed that an algorithm is involved in decisions
about them. The privacy notice doesn't mention AI or profiling at all.",
            "This fails the transparency requirement. Per ICO guidance, they
should tell people about AI use in clear language [61]. Not doing so violates
```

```
Art 13, and users can’t meaningfully exercise rights (Art 15) if they aren’t
aware."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["NO_EXPLANATION_OF_LOGIC"],
          "gdpr_refs": ["15(1)(h)", "22"],
          "rationale": [
            "Individuals receive a generic notice that “automated processing is
used,” but no meaningful information on logic or criteria. Article 15(1)(h)
requires providing meaningful information about the logic for solely automated
decisions.",

"While full algorithm transparency isn’t required, the current level of
information may be insufficient. This area needs review to improve
explainability (as ICO suggests via its explainability framework)."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["6(1)", "21"],
          "rationale": [
            "They have documented that initial model training uses legitimate
interests (with a completed LIA), and the deployed service uses consent from
users. These bases are listed in the privacy notice. So lawful bases are in
place for each processing context.",
            "Users are informed of these bases and can object or withdraw
consent accordingly. This separation of bases per phase aligns with ICO’s advice
 8  72 ."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["BIAS_OR_INACCURACY"],
          "gdpr_refs": ["5(1)(a)"],
          "rationale": [
            "No evidence of bias testing or fairness checks was provided. The
model was deployed without assessing if outcomes might favor or disfavor
protected groups.",
            "Unfair processing could violate Art 5(1)(a). Given ICO’s emphasis
on fairness and non-discrimination, the absence of any bias mitigation or human
review plan for high-stakes decisions is a failure of fairness."
          ]
        },
        {
          "expected_verdict": "PASS",
```

```
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(c)", "25(1)"],
          "rationale": [
            "The team minimized data – e.g., they truncated IP addresses and
removed names before training. They also only use features relevant to the
prediction. This demonstrates compliance with data minimization (Art 5(1)(c)).",
            "Privacy by design (Art 25) is evident: they even employed
differential privacy noise in training to reduce personal data impact. Such
measures show they're using the least data necessary."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["SECURITY_CONCERNS"],
          "gdpr_refs": ["32"],
          "rationale": [
            "Basic security like encryption at rest and access control exists,
but there's no indication of specific measures against AI-related risks (e.g.,
model inversion or membership inference attacks that could extract training
data).",
            "The security might be technically compliant, but given AI models'
unique risks, the sufficiency **needs review**. The ICO would expect considering
such AI-tailored security steps under Art 32."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["15", "16", "17", "21", "22"],
          "rationale": [
            "The organization has established channels for DSARs: individuals
can request their data and have it corrected or deleted. They demonstrate this
by providing a test user with a summary of their data and retraining the model
without that user's data upon deletion request.",
            "For automated decisions, they've implemented a right to human
review per Art 22(3) in the process. These steps show compliance with data
subject rights requirements."
          ]
        }
      ],
      "ambiguity_notes": "One challenge here is how much information is
"meaningful" when explaining AI logic to individuals. The ICO suggests giving
general explanation of factors and features, but there's still ambiguity on the
level of detail – too little isn't helpful, too much can be confusing or reveal
trade secrets. The guidance doesn't eliminate that judgment call. Also,
balancing technical security controls for AI (like preventing model inversion)
is new territory; the guidance flags it but practice is evolving. Finally,
determining fairness can be subjective – the ICO expects proactive bias checks,
```

```
but what metrics to use and what level of disparity is unacceptable isn't black-and-white in GDPR, leaning on equality law context."
    },
    {
      "id": "gs_008",
      "title": "Amsterdam Court (Netherlands) – Drivers vs. Uber & Ola (Algorithmic Management)",
      "authority": "District Court of Amsterdam",
      "jurisdiction": "Netherlands (EU)",
      "date": "2021-03-11",
      "source_url": "http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html",
      "excerpt": "In one case, the Court held that Ola's automated system for issuing driver *penalties and deductions* significantly affected drivers and thus triggered Article 22 GDPR [73] [74]. Ola was ordered to provide drivers with the *main assessment criteria and their role* in the automated decision, so drivers can understand on what basis they were penalized and check the processing's correctness [74]. In contrast, Uber's algorithmic matching of drivers to riders was not found to produce legal or similarly significant effects (the drivers hadn't shown a concrete impact) [75]. For Uber's account deactivations, the Court accepted Uber's explanation that a human ultimately decided (so Article 22 did not apply) [76]. However, the Court did fault Uber for not providing enough access to certain personal data and logic, emphasizing that *transparency and access rights extend to profiling data and meaningful information about algorithms*.",
      "ai_relevance_tags": ["automated_decision", "Article_22", "explanation", "transparency", "DSR_access", "ride_hailing"],
      "facts_summary": [
        "A group of ride-hailing drivers sued Uber and Ola, alleging they were subject to automated decisions (algorithmic management) without proper transparency, in breach of GDPR (Articles 15 and 22).",
        "The Amsterdam District Court issued three judgments. Key outcomes:",
        "– **Ola case**: Ola's system automatically imposed monetary penalties on drivers for certain "irregularities" (e.g., what it deemed fraudulent rides). The Court found this had a "similarly significant effect" on drivers (loss of income) [77], so Article 22(1) GDPR was engaged. Ola was thus obliged under Art 15(1)(h) to provide **meaningful information about the logic**. The Court ordered Ola to explain the main criteria its algorithm used for penalties [74].",
        "– **Uber employment case**: Drivers argued Uber's dispatch algorithm (which matches drivers to ride requests) and its performance monitoring amounted to automated decision-making affecting their work (e.g., impacting income). The Court ruled those particular processes did **not** meet the threshold of significant effect – drivers hadn't proven a legal or significant impact like denial of work or income from that specific algorithm [75]. Thus, Art 22 didn't apply there, and Uber didn't have to provide logic details under that article.",
        "– **Uber deactivation case**: Some drivers were deactivated (fired) allegedly by an algorithm (fraud detection). Uber said a human "Operational Risk" team reviewed the fraud flags and made the final call [78]. The Court
```

```
accepted this, so it wasn't a solely automated decision. Therefore, Article 22
protections did not formally apply. The drivers' request for the algorithm's
logic was denied because a human was in the loop (and drivers didn't contest
Uber's evidence of human involvement).",
        "Nonetheless, in all cases the Court reinforced that **Article 15(1)
(h)** gives a right to know meaningful information about any automated
processing (even if not solely automated). It was the first time a court
explicitly acknowledged a "right to an explanation" in GDPR terms [79]. Ola was
compelled to reveal its algorithmic criteria, and Uber was told to provide
additional data to drivers (like their personal ratings, etc.).",
        "This set of cases essentially clarifies that if an AI decision
significantly affects someone, they have a right to a human-interpretable
explanation of how that decision was made, and even when not fully automated,
transparency about profiling is expected."
      ],
      "questions": [
        "Does the AI or algorithm make decisions about individuals that have
legal or similarly significant effects (e.g. monetary penalties, account
termination, denial of services)? If so, are those decisions made solely by
automated means?",

"For any decision identified as fully automated and significant, has the data
subject been provided with meaningful information about the logic involved, as
required by GDPR (Article 15 and 22)?",
        "If the company claims a human is involved in the AI-driven decision
(thus avoiding Article 22's prohibition), is that human involvement real and
meaningful (not just a token review)?",
        "In the context of AI-driven decisions (even if not solely automated),
are individuals able to access data about their performance or profile that the
AI uses (under Article 15)?",
        "Has the organization implemented a process for individuals to contest
automated decisions or have a human review them, especially in cases of negative
outcomes like account suspension or penalties?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["22(1)"],
          "rationale": [
            "The AI's decisions (e.g., product recommendations) do not have
significant or legal effect on users – they're low-stakes. Therefore,
Article 22(1) is not triggered. There is no violation in using AI for these
minor decisions without explicit safeguards, as they don't materially affect
individuals' rights.",
            "Since no decision like firing, credit denial, or fines is made
solely by AI, the stringent requirements of Art 22 don't apply. This scenario is
compliant given the impact level."
```

```
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["AUTOMATED_DECISION_NO_EXPLANATION"],
          "gdpr_refs": ["22(3)", "15(1)(h)"],
          "rationale": [
            "The system auto-terminates user accounts for ‘fraud’ with no human
check and no explanation given. This is a **solely automated decision with
significant effect** (loss of service/income) but the users weren’t informed of
the logic.",

"That breaches Art 22(3) which requires safeguards like the right to obtain an
explanation and human intervention. Also, under Art 15(1)(h), individuals should
be able to get meaningful information on the algorithm’s criteria [74] – which the
company failed to provide."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["HUMAN_IN_LOOP_CLAIM"],
          "gdpr_refs": ["22(1)"],
          "rationale": [
            "The company states a human reviews AI decisions (like a manager
checks all flagged cases), but this is not well-documented. If the human review
is just a formality, the decision might effectively be automated.",
            "This situation needs closer review. If human involvement isn’t
meaningful – e.g., rubber-stamping AI outputs – regulators/courts could still
treat it as essentially automated. The organization should clarify and possibly
improve this process to ensure compliance."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["15"],
          "rationale": [
            "Individuals can access the data the AI uses about them: e.g.,
drivers can see their ratings, number of cancellations, etc. The company has a
portal or report for users to get their profile data.",
            "Providing this information meets Art 15 rights. In the Uber/Ola
case, lack of such access was an issue – here it’s resolved, so compliance is
achieved."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_CONTESTATION_PROCESS"],
```

```
          "gdpr_refs": ["22(3)"],
          "rationale": [
            "There is no channel for users to contest or appeal an AI-driven
decision (like account suspension). The policy says “AI decisions are final.”
This violates Art 22(3) which requires the ability to obtain human intervention
and contest the decision when Art 22 applies.",
            "Even if the company argues Art 22 doesn’t formally apply, it’s a
best practice (and arguably within fairness) to allow contestation for
significant automated outcomes. The absence of any review process is a red flag
for fairness and compliance."
          ]
        }
      ],
      "ambiguity_notes": "These rulings illustrate the fine line in determining
what is a “similarly significant effect.” The threshold isn’t crystal clear –
for example, how much income loss counts as significant? Courts may differ. It
also shows a pragmatic approach: if a company can show humans meaningfully
oversee an AI, Art 22 might not kick in, but what counts as meaningful oversight
is debated. The notion of a ‘right to explanation’ comes through via Art 15(1)
(h) and Art 22, but it’s not absolute – companies must give key criteria, not
full algorithms. There’s ambiguity in how detailed and how frequently such
explanations must be provided, left to case-by-case judgments."
    },
    {
      "id": "gs_009",
      "title": "CJEU – Österreichische Post (UI v. Austrian Post AG): Inferring
Political Leanings = Special Category Data",
      "authority": "Court of Justice of the EU (Grand Chamber)",
      "jurisdiction": "EU (Austria reference)",
      "date": "2023-05-04 (Judgment in Case C-300/21)",
      "source_url": "https://curia.europa.eu/juris/document/document.jsf?
text=&docid=260147",
      "excerpt": "The CJEU held that **inferring** a natural person’s probable
political opinions through data analysis constitutes processing of *special
category* personal data under Article 9(1) GDPR [80] [81]. Even though the
controller (Austrian Post) only generated a statistical likelihood of
affiliation to a political party, this still “reveals” political opinions about
the individual. As no explicit consent or other Article 9(2) condition was
obtained, this processing was unlawful. The case clarified there is no
“accuracy” or insignificance threshold to escape Article 9 – any profiling that
targets sensitive attributes falls under the special data rules. (The judgment
also addressed compensation for GDPR breaches, finding that a mere breach does
not automatically entitle damages without concrete harm, but that’s separate
from the AI issue.)",
      "ai_relevance_tags": ["profiling", "special_category", "inference",
"political_opinion", "lawful_basis"],
      "facts_summary": [
```

```
        "Austrian Post profiled citizens for marketing purposes. Using various
demographic data, it algorithmically assigned each person a probability of
supporting a particular political party. One individual (UI) sued, objecting
that this unwarrantedly attributed him a political view, causing distress.",
        "Key point: No political opinion was directly collected – it was
**inferred** via analytics. Austrian Post did not treat this as sensitive data
processing, and did not have consent or a valid Art 9(2) basis.",

"The CJEU was asked if such inferred data is “special category” data. It ruled
*yes*: inferring someone’s likely political affinity “reveals” their political
opinions within the meaning of GDPR Article 9(1) [80]. It rejected arguments that
only certain or explicitly stated opinions count. Even a probability or
marketing classification about politics triggers Article 9.",
        "Therefore, controllers cannot evade the strict rules on sensitive data
by saying “it’s just a prediction” – the nature of the attribute (political
opinion) matters, not how certain the inference is.",
        "As Austrian Post had no Art 9(2) exception (like explicit consent) for
this processing, it was unlawful. The Austrian courts had already issued an
injunction stopping the profiling.",
        "The judgment also noted (obiter) that data subjects suffering non-
material harm (like distress at being profiled politically) could claim
compensation if damage is proven, and that breaches must cause harm to get
damages (no automatic damages for any breach). But importantly for AI: any AI
profiling that targets things like health, sex life, political or religious
views, etc., will be seen as processing sensitive data, requiring heightened
safeguards.",
        "This influences AI model training and outputs: e.g., if an AI infers
someone’s religion or sexual orientation from browsing data, that output is
sensitive data and GDPR Art 9 applies.",
        "It underscores that even derived or inferred data isn’t exempt from
GDPR categories – content matters more than provenance in classification."
      ],
      "questions": [
        "Does the AI system derive or infer any attributes about individuals
that fall under special categories (e.g. inferring political views, religious
beliefs, health status) from otherwise non-sensitive data?",
        "If yes, has the organization obtained explicit consent for this
profiling or otherwise met an Article 9(2) condition allowing processing of
those inferred special categories?",
        "Were individuals made aware that such sensitive inferences would be
made about them, and given the opportunity to object or opt-out?",
        "Does the organization treat inferred sensitive traits with the same
care as provided data? For example, if the model predicts someone’s ethnicity or
orientation, is that handled under GDPR’s special data rules (with higher
protection and lawful basis)?",
        "Has the organization evaluated the model to ensure it’s not
inadvertently producing special category data from the input (for instance, by
correlating data points that reveal health or beliefs)? If it does, are those
```

```
outputs immediately protected or minimized?"
      ],
      "expected_answers": [
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["SPECIAL_CATEGORY_INFERENCE",
"NO_CONDITION_FOR_SENSITIVE"],
          "gdpr_refs": ["9(1)", "9(2)"],
          "rationale": [
            "Yes, the AI's profiling tool assigns individuals a "suspected
political leaning" score without consent. That is processing of political
opinion data [80]. Without an Art 9(2) exemption (like explicit consent), this is
unlawful.",
            "As per CJEU, even inferred probabilities count as sensitive data.
The company neither sought consent nor had legal authority, violating Art 9(1)."
          ]
        },
        {
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
          "gdpr_refs": ["13", "5(1)(a)"],
          "rationale": [
            "Individuals were not informed that the service would infer
sensitive traits about them. The privacy notice did not mention political
opinion profiling.",
            "This lack of transparency compounds the issue – people didn't even
know to consent or object. It's a breach of Art 13 and the fairness principle."
          ]
        },
        {
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["POTENTIAL_SPECIAL_DATA"],
          "gdpr_refs": ["9(1)", "25(1)"],
          "rationale": [

"The organization didn't initially realize their AI outputs might be sensitive
data. Now that this ruling exists, they need to review their model's outputs.",
            "It's possible the AI indirectly infers health or other special
categories (e.g., through correlations). A review is needed to check if any
outputs fall under Art 9 and if so, to implement appropriate safeguards or stop
those inferences."
          ]
        },
        {
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["25(1)", "5(1)(c)"],
          "rationale": [
```

```
            "The AI model was intentionally designed not to profile or output
any sensitive attribute. It only predicts generic preferences that are not in
Art 9 categories.",
            "This privacy-by-design choice (avoiding special categories
altogether) means Art 9 is not engaged. By minimizing data attributes to exclude
sensitive ones, they stay compliant and avoid needing extra conditions."
          ]
        }
      ],
      "ambiguity_notes": "This decision firmly establishes that **inferences =
data** in GDPR terms, resolving some debate. However, it raises practical
questions: How should companies handle inadvertent sensitive inferences? For
example, if an AI analysis unintentionally correlates to health (like an AI that
predicts depression risk from typing patterns), does that trigger Art 9? The
answer seems yes, but companies might not even realize when it's happening. The
judgment suggests erring on the side of caution. It also leaves open how
"probabilistic" an inference must be – but essentially any targeted inference
about a sensitive trait qualifies, regardless of accuracy. Organizations now
must consider even derived data in their GDPR scoping, which can be challenging
if those inferences are deep in model logic."
    },
    {
      "id": "gs_010",
      "title": "EDPB Guidelines on Virtual Voice Assistants (2021) – Data
Protection in Voice AI",
      "authority": "EDPB",
      "jurisdiction": "EU",
      "date": "2021-07-07 (final version)",
      "source_url": "https://www.edpb.europa.eu/our-work-tools/our-documents/
guidelines/guidelines-022021-virtual-voice-assistants_en",
      "excerpt":
"Many VVA services store voice commands and other personal data until users
delete them – this conflicts with the *storage limitation* principle. VVAs
should not retain personal data longer than necessary for the purpose [57]. For
example, raw voice recordings that have been processed into text should be
deleted once no longer needed for the request. The guidelines also stress data
minimization: voice assistants should implement techniques to avoid recording
ambient conversations or other voices (e.g. via on-device wake word detection)
[82] [83]. Users must be informed (Article 13) at device setup or first use that
their voice inputs will be processed and possibly stored, and given options like
muting or deleting recordings [84].",
      "ai_relevance_tags": ["voice_assistant", "audio", "data_retention",
"data_minimization", "transparency", "special_category", "DPIA"],
      "facts_summary": [
        "These guidelines cover AI-driven **Virtual Voice Assistants** (VVAs)
like Siri, Alexa, etc., which use speech recognition and natural language
processing. They highlight GDPR issues and give recommendations:",
        "– **Transparency & Consent**: Often, activation of a voice assistant
```

leads to continuous listening. Users (and anyone whose voice might be captured) should be informed that audio data is being processed. If VVAs process sensitive data via voice (like health info in a query), explicit consent might be needed in some contexts. Parental consent is needed if children's voices are recorded for non-necessary processing.",

"- **Data Protection by Design**: Voice assistants should be designed to **minimize unintended capture**. For instance, device-side detection of wake-words to avoid sending all audio to cloud; automatically turning off microphone when not needed; options for users to deactivate listening.",
"- **Minimization**: Don't collect more audio or metadata than necessary. E.g., don't continuously upload## Dataset Entries

```json
{
  "dataset": [
    {
      "id": "gs_001",
      "title": "WP29/EDPB Guidelines on Automated Decision-Making and Profiling",
      "authority": "Article 29 Working Party (endorsed by EDPB)",
      "jurisdiction": "EU",
      "date": "6 February 2018",
      "source_url": "https://ec.europa.eu/newsroom/article29/items/612053",
      "excerpt":
"Profiling may identify special categories of data by inference (for example inferring an individual's state of health from records of their food shopping). The controller must also satisfy the conditions in Article 9(2) for special categories of data inferred from profiling [1].",
      "ai_relevance_tags": ["automated_decision", "profiling", "special_category", "transparency", "lawful_basis"],
      "facts_summary": [
        "Defines profiling and automated decisions under GDPR and their risks.",

"Confirms that inferring sensitive data (like health, political beliefs) from otherwise non-sensitive data counts as processing special category data, requiring an Article 9(2) condition [1].",
        "Emphasizes transparency: individuals must be informed about profiling and their right to object [2].",

"Stresses need for lawful basis for all profiling; consent or legitimate interests must be carefully assessed [3].",

"Highlights controllers' obligations to implement safeguards (like human review for impactful automated decisions) and ensure data minimization, accuracy, fairness in profiling outcomes."
      ],
      "questions": [
```

```
        "If an AI system profiles users to infer health status or political
views, has the system obtained explicit consent or another Article 9(2)
condition for processing this inferred sensitive data?",
        "When using automated profiling that significantly affects individuals,
does the system provide meaningful information about the logic involved and
ensure human intervention upon request?"
      ],
      "expected_answers": [
        {
          "question": "If an AI system profiles users to infer health status or
political views, has the system obtained explicit consent or another Article
9(2) condition for processing this inferred sensitive data?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["SPECIAL_DATA_NO_CONDITION",
"NO_LAWFUL_BASIS"],
          "gdpr_refs": ["9"],
          "rationale": [

"The guidelines note that inferring special categories (e.g. health) from other
data brings the processing under Article 9 [1] . Not having an explicit consent or
other exception would violate GDPR.",
            "If no explicit consent (or other Art.9 basis) was obtained for
processing inferred sensitive data, the processing lacks a lawful basis [1] . This
constitutes unlawful processing of special category data."
          ]
        },
        {
          "question":
"When using automated profiling that significantly affects individuals, does the
system provide meaningful information about the logic involved and ensure human
intervention upon request?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["13", "14", "22"],
          "rationale": [
            "WP29 guidance requires that individuals are informed about
automated decision-making, including meaningful information about the logic
involved.",
            "Controllers must implement safeguards such as human review for
significant automated decisions. Providing these safeguards and explanations
would meet GDPR obligations.",
            "If the system can explain its profiling decisions and allows users
to contest or obtain human intervention, it aligns with Articles 13–15 and 22
requirements, thus no violation signal is present."
          ]
        }
      ],
      "ambiguity_notes": "The guidelines introduce a 'right to explanation'
```

```
debate. While not explicitly in the GDPR text, WP29 interprets Articles 15 and
22 as requiring meaningful information about algorithmic logic. However, what
level of detail satisfies 'meaningful information' is somewhat open to
interpretation, as is the extent to which trade secrets limit disclosure."
    },
    {
      "id": "gs_002",
      "title": "EDPB Report on the ChatGPT Task Force (Interim Results)",
      "authority": "European Data Protection Board",
      "jurisdiction": "EU",
      "date": "23 May 2024",
      "source_url": "https://edpb.europa.eu/system/files/2024-05/
edpb_20240523_report_chatgpt_taskforce_en.pdf",
      "excerpt": "When web scraping personal data from publicly accessible
sources, the requirements of Article 14 GDPR apply. Considering large amounts of
data is collected via web scraping, it is usually not practicable or possible to
inform each data subject...Therefore, the exemption pursuant Article 14(5)(b)
GDPR could apply, as long as all requirements of this provision are fully met.
Contrary to this, when personal data is collected while directly interacting
with ChatGPT, the requirements of Article 13 GDPR apply. In this context, it is
of particular importance to inform data subjects that the user input may be used
for training purposes [13].",
      "ai_relevance_tags": ["model_training", "web_scraping", "transparency",
"data_accuracy", "DSR_access", "DSR_rectification"],
      "facts_summary": [
        "EDPB formed a Task Force to coordinate national investigations into
ChatGPT and similar LLM services.",
        "The report emphasizes transparency obligations: if personal data are
scraped from the web to train an AI, controllers should normally provide
Article 14 notices unless a 14(5)(b) exemption (disproportionate effort)
strictly applies.",
        "For data collected directly from users (prompts, chats), Article 13
notice must be given at collection, including that user inputs may be used to
improve/train the model [13].",

"Highlights the data accuracy principle: ChatGPT outputs may be false or
fabricated; nonetheless, controllers must address inaccuracies, especially when
output pertains to individuals.",

"Notes difficulties in honoring data subject rights (like rectification) in
LLMs. OpenAI suggested erasure as a substitute for rectification. The report
stresses controllers should facilitate all GDPR rights (access, erasure,
objection, etc.) despite technical challenges.",
        "Calls for privacy by design: incorporating measures to enable deletion
or correction of personal data in training sets and to prevent disproportionate
impacts on individuals (e.g. unfair or misleading outputs) [20]."
      ],
      "questions": [
```

```
        "If the AI model is trained on personal data scraped from websites, has
the organization provided data subjects with an Article 14 notice or properly
justified an exemption under Art 14(5)(b)?",
        "Does the service inform users at sign-up or input time that their
prompts and content may be used for model training, in compliance with
Article 13 transparency requirements?",
        "Can individuals have inaccurate or harmful personal data produced by
the chatbot corrected or deleted, and are mechanisms in place to facilitate
their data subject rights (e.g. access, erasure)?"
      ],
      "expected_answers": [
        {
          "question": "If the AI model is trained on personal data scraped from
websites, has the organization provided data subjects with an Article 14 notice
or properly justified an exemption under Art 14(5)(b)?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["NO_ART14_NOTICE",
"UNVERIFIED_14-5b_EXEMPTION"],
          "gdpr_refs": ["14"],
          "rationale": [
            "The EDPB report notes that when personal data is scraped for
training, Article 14 obligations apply unless a narrow exemption is met.",
            "If the organization did not attempt to inform data subjects and
simply assumed the Art 14(5)(b) 'disproportionate effort' exemption, this needs
careful review. The exemption is only valid if *all* conditions are met – which
is a high bar (e.g. truly impossible to inform, and processing must be in public
interest, etc.).",
            "A lack of any notice to millions of data subjects would signal
potential non-compliance with Article 14, unless robust evidence shows the
exemption conditions are satisfied. This merits further investigation rather
than a clear pass."
          ]
        },
        {
          "question": "Does the service inform users at sign-up or input time
that their prompts and content may be used for model training, in compliance
with Article 13 transparency requirements?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["13", "5(1)(a)"],
          "rationale": [
            "The report specifies that for data collected directly from users
(e.g. prompts), Article 13 information must be provided, particularly that user-
provided content may be used for training [13] .",
            "If the service clearly notifies users (e.g. in a privacy notice or
at the chat interface) that their inputs can be used to improve the model, this
satisfies the transparency requirement. Many services added such disclosures
after regulatory scrutiny.",
```

```
            "Assuming the service implemented enhanced transparency (as OpenAI
did post-Italy ban), there would be no signal of violation here."
          ]
        },
        {
          "question": "Can individuals have inaccurate or harmful personal data
produced by the chatbot corrected or deleted, and are mechanisms in place to
facilitate their data subject rights (e.g. access, erasure)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["DSR_OBSTRUCTION",
"NO_RECTIFICATION_MECHANISM"],
          "gdpr_refs": ["15", "16", "17", "22"],
          "rationale": [
            "EDPB noted that OpenAI did not offer a means to rectify incorrect
personal data about individuals produced by ChatGPT, instead suggesting deletion
due to technical difficulty [17] .",

"The right to rectification (Art 16) and to erasure (Art 17) must be practical.
If the model can output personal data, the controller should have a process to
remove or update that data in future outputs. Not having any feasible mechanism
to correct AI-generated false information about someone is a GDPR red flag.",
            "In the absence of robust user-rights processes (automated or
manual) to handle removals and access requests, the system fails to fully comply
with GDPR's data subject rights. The need for human intervention in automated
decisions (Art 22(3)) also implies a mechanism should exist to review and
rectify outputs about individuals."
          ]
        }
      ],
      "ambiguity_notes": "There is uncertainty on how to implement certain
rights in AI systems. For example, the right to rectification is technically
challenging if a model has 'learned' incorrect data. The report implies deletion
may be an acceptable mitigation, but it leaves open questions on feasibility.
Additionally, reliance on the Article 14(5)(b) exemption for web-scraped data is
ambiguous – DPAs may differ on what constitutes disproportionate effort in the
AI training context."
    },
    {
      "id": "gs_003",
      "title": "Italian Garante vs. OpenAI – ChatGPT Temporary Ban",
      "authority": "Garante (Italian Data Protection Authority)",
      "jurisdiction": "Italy",
      "date": "31 March 2023 (interim order), 28 April 2023 (service
reinstated)",
      "source_url": "https://www.garanteprivacy.it/home/docweb/-/docweb-display/
docweb/9870847",
      "excerpt": "The Italian SA found that OpenAI had no legal basis for the
mass collection and processing of personal data to train the ChatGPT model, and
```

```
that it provided no notice to users or data subjects whose data were scraped. Additionally, no age verification measures were in place to protect minors. The SA imposed a temporary ban on ChatGPT's data processing in Italy until OpenAI addressed these issues [27].",
      "ai_relevance_tags": ["model_training", "web_scraping", "transparency", "lawful_basis", "children_protection", "DSR_erasure"],
      "facts_summary": [
        "On 31 March 2023, Garante issued an emergency order halting ChatGPT in Italy due to GDPR violations.",
        "The DPA observed OpenAI had *no disclosed legal basis* for processing personal data scraped from the internet to train the model (no consent or other explicit basis).",

"It noted a lack of transparency: individuals (non-users) whose data was included in training were not informed, and users were not adequately informed about data use. The privacy notice was found insufficient.",
        "No age verification: ChatGPT had no filter to prevent users under 13 (or under 18) from using the service, exposing minors' data without parental consent [27].",
        "Garante also highlighted potential inaccuracies in ChatGPT outputs (hallucinations about people) indicating breaches of data accuracy and the inability of data subjects to correct or erase their data.",
        "OpenAI responded by adding an age-gate, improving privacy notices, providing an opt-out form for data, and other measures. The service was reinstated on 28 April 2023 after OpenAI implemented preliminary remedies. A later investigation (2023–24) resulted in a €5 million fine and a requirement for a public awareness campaign."
      ],
      "questions": [
        "Did the company have a valid GDPR legal basis (e.g. consent or legitimate interests) for using personal data scraped from the internet to train the AI model?",
        "Did the service provide clear and sufficient privacy notices to users and non-users, informing them that their personal data (including prompts or public data) would be collected and used for training purposes?",
        "Were effective measures in place to prevent children under the age threshold from using the AI service and having their personal data processed (e.g. age verification)?",
        "Does the service offer a way for individuals to request deletion of their personal data from the model (or otherwise exercise their GDPR rights), given the model might output personal information inaccurately?"
      ],
      "expected_answers": [
        {
          "question": "Did the company have a valid GDPR legal basis (e.g. consent or legitimate interests) for using personal data scraped from the internet to train the AI model?",
          "expected_verdict": "FAIL",
```

```
          "expected_violation_signals": ["NO_LAWFUL_BASIS"],
          "gdpr_refs": ["5(1)(a)", "6"],
          "rationale": [
            "The Garante found no appropriate legal basis for OpenAI's
processing of personal data for training ChatGPT. OpenAI did not obtain consent
from data subjects, nor did it successfully invoke another Article 6 basis.",
            "Scraping personal data en masse without informing individuals or
establishing a lawful basis violates the principle of lawfulness and fairness
(Art 5(1)(a)). The Italian DPA's order was predicated on this fundamental
failure.",
            "Without a lawful basis, any processing of personal data is
inherently unlawful under GDPR. Thus, the usage of scraped data for model
training was deemed in breach of Articles 5 & 6."
          ]
        },
        {
          "question": "Did the service provide clear and sufficient privacy
notices to users and non-users, informing them that their personal data
(including prompts or public data) would be collected and used for training
purposes?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
          "gdpr_refs": ["5(1)(a)", "12", "13", "14"],
          "rationale": [
            "The Italian DPA identified an absence of proper transparency.
Affected individuals whose data was scraped had received no notice (violating
Article 14). Users, too, were not adequately informed at sign-up that their
prompts could be retained for training.",
            "GDPR Articles 13–14 require that data subjects be informed about
the collection and use of their personal data. OpenAI's privacy notice was found
to be lacking in this regard, prompting the DPA to mandate improved
disclosures.",
            "Because neither users nor third-party data subjects were properly
informed, the service fell short of GDPR transparency obligations. The lack of
an intelligible, accessible notice about training-data usage signaled a clear
transparency failure."
          ]
        },
        {
          "question": "Were effective measures in place to prevent children
under the age threshold from using the AI service and having their personal data
processed (e.g. age verification)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["CHILDREN_UNPROTECTED"],
          "gdpr_refs": ["5(1)(a)", "8"],
          "rationale": [
            "Garante explicitly called out the *absence of age verification* as
a violation [27]. ChatGPT had no checks to block underage users, despite
```

```
processing personal data and even sensitive content.",
            "Article 8 GDPR requires parental consent for information society services offered to children under 16 (or lower age defined by member state, 13 in Italy). By not verifying age, OpenAI could be unknowingly processing data of minors without consent, contravening child data protection rules.",
            "The lack of any age gating meant minors' data could be collected and used in training. This was a key issue in the ban; OpenAI's later implementation of a rudimentary age check was an attempt to remedy this. Without such measures initially, the service failed to comply with GDPR's fairness and lawfulness principles regarding children."
          ]
        },
        {
          "question": "Does the service offer a way for individuals to request deletion of their personal data from the model (or otherwise exercise their GDPR rights), given the model might output personal information inaccurately?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["DSR_ERASURE_LIMITED"],
          "gdpr_refs": ["17", "12"],
          "rationale": [
            "Initially, ChatGPT had no user-facing mechanism for data subjects to request erasure or correction of personal data contained in training data or outputs. The Garante demanded OpenAI provide a way for Europeans (users and non-users) to request deletion of their personal data.",
            "OpenAI rapidly stood up a web form for data erasure requests as part of compliance measures. However, the effectiveness of this process (and whether it truly deletes all instances of one's data from the model) remains uncertain. The DPA's final orders included requiring simplified rights exercises and even a public awareness campaign on these rights.",
            "Given these uncertainties, this is marked 'Needs Review'. If an audit finds that the deletion process is unclear or ineffective (e.g., only removing chat history but not the trained model data), it would indicate ongoing GDPR compliance issues. Proper evaluation of the implemented rights mechanism is needed to decide pass/fail."
          ]
        }
      ],
      "ambiguity_notes": "This case underscored new challenges applying GDPR to generative AI. For example, how to allow erasure from a trained model is technically ambiguous. The legality of scraping public data for AI training under 'legitimate interests' remains debated – OpenAI did not attempt a balancing test before launch. Additionally, age verification standards are not clearly defined: OpenAI added a simple age gate, but the sufficiency of that (absent robust identity verification) is debatable under GDPR."
    },
    {
      "id": "gs_004",
      "title": "CNIL (France) – Clearview AI Facial Recognition Sanction",
```

```
      "authority": "CNIL (French Data Protection Authority)",
      "jurisdiction": "France",
      "date": "17 October 2022 (final decision)",
      "source_url": "https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai",
      "excerpt": "The CNIL's Restricted Committee found that Clearview AI had collected and used the facial images of individuals in France without any legal basis (Art.6), failed to provide notice or honor rights (Arts.12, 15, 17), and unlawfully processed sensitive biometric data. CNIL imposed a €20 million fine and ordered Clearview to cease processing data of people in France and delete existing data.",
      "ai_relevance_tags": ["facial_recognition", "model_training", "biometrics", "lawful_basis", "DSR_access", "DSR_erasure", "transparency"],
      "facts_summary": [
        "Clearview AI scraped billions of facial images from the internet (social media, websites) to build a facial recognition AI database. Individuals were not informed and did not consent.",
        "CNIL received complaints and issued a formal notice in 2021; Clearview ignored it. Consequently, CNIL's Restricted Committee issued a sanction in 2022.",
        "Key GDPR violations found: **Unlawful processing (no valid legal basis)** for collecting and using facial images (breach of Art.6) [36]; **Processing of sensitive biometric data without consent** (faces are biometric data under GDPR); **Lack of transparency and notice** – data subjects (including those never using Clearview) were not informed (Arts.12, 14); **Failure to honor rights** – Clearview did not facilitate access or deletion requests (Arts.15, 17) [36].",

"Clearview also failed to cooperate with CNIL (Art.31) by not responding to the formal notice.",
        "Sanctions: €20 million fine (max for GDPR in France) and an order to stop collecting and processing faces of people in France without legal basis, and to delete existing images within 2 months [35] (with heavy penalty fines for non-compliance per day).",
        "This case set a precedent that scraping publicly available photos for facial recognition is subject to GDPR and requires compliance with lawful basis, transparency, and data subject rights."
      ],
      "questions": [

"Did the company obtain a valid GDPR legal basis (e.g. explicit consent) for collecting and using individuals' facial images from the internet for its facial recognition database?",
        "Did the company inform individuals in a clear and accessible way that it was processing their photos for facial recognition, and did it facilitate their rights (such as access or deletion of their data)?",

"Is the processing of biometric facial data limited to what is necessary and
```

```
lawful (with an appropriate Article 9(2) condition), and are there measures to
prevent indefinite retention of this data?"
      ],
      "expected_answers": [
        {
          "question": "Did the company obtain a valid GDPR legal basis (e.g.
explicit consent) for collecting and using individuals' facial images from the
internet for its facial recognition database?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS",
"SPECIAL_DATA_NO_CONDITION"],
          "gdpr_refs": ["6", "9"],
          "rationale": [
            "The CNIL concluded Clearview had *no legal basis* for its massive
data scraping – individuals never consented and no other Art.6 basis was
applicable [36].",
            "Biometric data (facial recognition templates) are special category
data under GDPR. Clearview did not have an Art.9(2) condition (like explicit
consent) for processing this sensitive data. Thus, the processing was unlawful
on two counts: no Art.6 basis and no Art.9 basis.",
            "Without consent or another lawful ground, the collection of
billions of images was inherently illegal. CNIL's fine and order were predicated
on this fundamental violation of GDPR's lawful processing requirements."
          ]
        },
        {
          "question": "Did the company inform individuals in a clear and
accessible way that it was processing their photos for facial recognition, and
did it facilitate their rights (such as access or deletion of their data)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY",
"DSR_NOT_HONORED"],
          "gdpr_refs": ["12", "14", "15", "17"],
          "rationale": [
            "Clearview provided no privacy notice to the millions of people in
its database. Affected individuals (whose images were scraped) were unaware –
violating Articles 12 and 14's transparency duties [36].",
            "When some individuals tried to exercise access or deletion,
Clearview reportedly did not comply (one of the reasons CNIL cited breaches of
Arts.15 and 17) [36]. CNIL noted individuals' rights were not respected.",
            "Because data subjects were neither informed nor given effective
means to control their data, Clearview blatantly failed GDPR transparency and
data subject rights obligations. The enforcement notice explicitly required
Clearview to establish procedures for access and erasure requests, underscoring
that such mechanisms were missing."
          ]
        },
        {
```

```
          "question": "Is the processing of biometric facial data limited to
what is necessary and lawful (with an appropriate Article 9(2) condition), and
are there measures to prevent indefinite retention of this data?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["EXCESSIVE_DATA_COLLECTION",
"UNLIMITED_RETENTION"],
          "gdpr_refs": ["5(1)(c)", "5(1)(e)", "9"],
          "rationale": [
            "Clearview amassed a huge database of every photo it could find –
this indiscriminate collection is the opposite of data minimization (Art.5(1)
(c)). CNIL found the data collection “massive and intrusive”, far beyond
necessity.",
            "There was no indication Clearview ever deleted any data; it aimed
to create a perpetual, growing database. Such indefinite retention without
periodic purge violates the storage limitation principle (Art.5(1)(e)).",
            "Coupled with the lack of a lawful basis for sensitive biometric
data, these practices show Clearview’s processing was neither necessary nor
proportionate. The fine and order to delete data reflect that the company’s
approach breached core GDPR principles of limitation and necessity."
          ]
        }
      ],
      "ambiguity_notes": "This case was straightforward in GDPR terms despite
Clearview’s absence in the EU. It affirmed that GDPR applies extraterritorially
when services target or involve EU individuals. One ambiguity is enforcement:
Clearview had no EU establishment and ignored orders. This raises questions
about how such deletion orders can be enforced in practice. Additionally, it
underscored debate on whether biometric templates from public photos are
“special category” data – CNIL treated them as such, requiring strict
conditions."
    },
    {
      "id": "gs_005",
      "title": "Italian Garante – Clearview AI Ban and Fine",
      "authority": "Garante (Italian Data Protection Authority)",
      "jurisdiction": "Italy",
      "date": "10 February 2022 (decision)",
      "source_url": "https://www.garanteprivacy.it/home/docweb/-/docweb-display/
docweb/9751308",
      "excerpt": "The Italian SA found several infringements by Clearview AI
Inc.: personal data, including biometric and geolocation information, were
processed unlawfully without an appropriate legal basis – the company’s claimed
legitimate interest does not qualify. Additionally, the company breached
fundamental principles of transparency, purpose limitation, and storage
limitation; it failed to provide the information required by Articles 13-14, to
respond to access requests (Art.15) in time, and to designate an EU
representative [39].",
      "ai_relevance_tags": ["facial_recognition", "biometrics", "lawful_basis",
```

```
"transparency", "purpose_limitation", "data_retention", "DSR_access"],
      "facts_summary": [
        "The Garante investigated Clearview in 2021 after reports on its facial recognition tool. In March 2022, it fined Clearview €20 million (the maximum) and issued sweeping corrective orders [46].",
        "**Unlawful processing:** Clearview claimed a ‘legitimate interest’ for scraping and using images, but the DPA held this was invalid for such intrusive processing. There was no proper legal basis (Art.6) for collecting Italians’ biometric and geolocation data. Special category data (biometric) was processed without meeting any Art.9 condition.",

"**Principle violations:** Clearview violated transparency (no notice to individuals, breaching Arts.13/14) and purpose limitation (using photos for an unrelated new purpose) [43]. It also violated storage limitation, keeping data indefinitely.",
        "Clearview failed to respond to data access requests within the legal timeframe, infringing Art.15 [45].",
        "The company had not appointed an EU representative (required under Art. 27 for a non-EU controller targeting EU data) [37].",
        "Orders: Beyond the fine, Garante banned any further scraping of images of people in Italy and any further use of Italian residents’ biometric data. It ordered Clearview to delete all existing data on Italian individuals and to designate an EU representative [47]."
      ],
      "questions": [
        "Did the company have a valid GDPR legal basis for collecting and processing Italians’ facial images (was ‘legitimate interest’ an acceptable ground in this context)?",
        "Did the company comply with the GDPR principles of transparency and purpose limitation when repurposing people’s online photos for facial recognition?",
        "Did the company implement data minimization and storage limitation (i.e., collect only necessary data and not retain it indefinitely)?",
        "Did the company fulfill its obligations to respond to data subject access requests and designate an EU representative as required?"
      ],
      "expected_answers": [
        {
          "question": "Did the company have a valid GDPR legal basis for collecting and processing Italians’ facial images (was ‘legitimate interest’ an acceptable ground in this context)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_LAWFUL_BASIS"],
          "gdpr_refs": ["6", "9"],
          "rationale": [
            "The Italian DPA flatly rejected Clearview’s claim of legitimate interest as a legal basis. The processing was too intrusive to rely on anything other than explicit consent or a similarly strong basis, which Clearview did not
```

```
have.",
            "Because biometric data was involved, an Article 9(2) condition was also needed. Clearview had none. Thus, there was no lawful basis under Art.6, nor any exemption under Art.9 – a fundamental GDPR breach.",
            "In summary, Clearview's operations in Italy lacked any valid legal ground. The enforcement – max fine and ban – hinged on this complete absence of a lawful basis."
          ]
        },
        {
          "question": "Did the company comply with the GDPR principles of transparency and purpose limitation when repurposing people's online photos for facial recognition?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY", "PURPOSE_CREEP"],
          "gdpr_refs": ["5(1)(b)", "12", "14"],
          "rationale": [
            "Clearview's use of people's photos (often from social media) for a new purpose (face search engine) was unrelated to the photos' original context – a clear breach of purpose limitation (Art.5(1)(b)). Individuals uploaded photos for personal/social use, not for a facial recognition database.",

"Transparency was nonexistent: individuals in Italy weren't informed that their images were being processed by Clearview [43]. No privacy notice was provided (violating Arts.12–14). The DPA explicitly found transparency failures.",
            "This repurposing of data, done covertly, represents "purpose creep." Because Clearview neither obtained fresh consent nor provided notice for the new use, it violated core principles. The enforcement orders requiring cessation and notice reflect this finding."
          ]
        },
        {
          "question": "Did the company implement data minimization and storage limitation (i.e., collect only necessary data and not retain it indefinitely)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["EXCESSIVE_DATA_COLLECTION", "UNLIMITED_RETENTION"],
          "gdpr_refs": ["5(1)(c)", "5(1)(e)"],
          "rationale": [
            "The Garante found Clearview infringed both data minimization and storage limitation principles [43]. It collected massive amounts of data (billions of images, plus metadata like geolocation) – far beyond what is necessary for any reasonable purpose.",

"Clearview also apparently kept data indefinitely. There was no data retention schedule; the service aimed to continually grow its database. This violates Art. 5(1)(e), which requires data not be kept longer than necessary.",
            "Because of these issues, the Italian DPA's order mandated deletion
```

```
of existing data and banned further collection. These remedies underscore that Clearview's practices were fundamentally at odds with GDPR's limits on scope and duration of data processing."
          ]
        },
        {
          "question": "Did the company fulfill its obligations to respond to data subject access requests and designate an EU representative as required?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["DSR_NOT_HONORED", "NO_EU_REPRESENTATIVE"],
          "gdpr_refs": ["15", "27"],
          "rationale": [
            "Clearview failed to timely honor individuals' access requests (Art. 15), as noted by the Garante [45]. People who asked for their data or for deletion either got no response or not within the legal timeframe. This non-compliance with DSAR obligations was part of the violations.",
            "Clearview had no establishment in the EU and had not appointed an EU representative under Article 27 [37], despite clearly operating in the EU market (offering services to European law enforcement, etc.). Failing to have an EU rep is itself a GDPR violation for an overseas controller processing EU data.",
            "These procedural and governance failures (ignoring user rights and ignoring Article 27 requirements) compounded the substantive violations. They illustrate a broad disregard for GDPR obligations, justifying the maximum sanctions imposed."
          ]
        }
      ],
      "ambiguity_notes": "The Clearview cases raised little ambiguity in interpretation – the violations were clear-cut. One notable aspect is jurisdiction: Clearview is a US company with no EU office. Enforcing deletion or fines is challenging, raising questions about cross-border enforcement efficacy. Additionally, defining the exact scope of 'biometric data' in scraped images could be debated (Clearview claimed it doesn't store raw photos, only embeddings). The DPAs nonetheless treated the embeddings as biometric personal data."
    },
    {
      "id": "gs_006",
      "title": "CNIL Guidelines – How to Develop AI Systems in Compliance with GDPR",
      "authority": "CNIL (France)",
      "jurisdiction": "France/EU",
      "date": "7 June 2024",
      "source_url": "https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr",
      "excerpt": "An AI system based on the exploitation of personal data must
```

```
be developed with a “purpose”, i.e. a well-defined objective. This makes it possible to frame and limit the personal data that can be used for training, so as not to store and process unnecessary data. The objective must be determined as soon as the project is defined, explicit to users, and legitimate. The CNIL considers that the requirement to define a purpose applies even for general-purpose AI – it must be adapted to the context of AI without disappearing [49] [50] .",
      "ai_relevance_tags": ["purpose_limitation", "data_minimization", "lawful_basis", "data_retention", "DPIA", "transparency", "privacy_by_design"],
      "facts_summary": [
        "The CNIL’s 2024 guidance is a practical 7-step roadmap for AI developers to integrate GDPR from the design phase [52] . It covers defining purpose, assigning roles, choosing a legal basis, data minimization, managing reuse of data, setting retention periods, and conducting DPIAs.",
        "Developers should **define a specific purpose** for the AI at the project outset (Art.5(1)(b)). Even if developing a general-purpose model, the guidance says you must articulate a use-case or range of uses to avoid open-ended data use [49] [50] .",
        "Data collected for training should be limited to what is necessary for that purpose (**data minimization**, Art.5(1)(c)). Avoid ingesting extraneous personal data. CNIL gives examples and emphasizes purpose helps determine necessity.",
        "Controllers must identify an appropriate **legal basis** (Art.6) for each stage (training vs. deployment) [8] [9] . For instance, training might rely on legitimate interest (if balanced and documented) while deployment might require consent, depending on context.",
        "If reusing data originally collected for another purpose, assess compatibility or seek new consent (avoid purpose creep) [54] . CNIL stresses checks before using previously gathered data for AI training (Step 4).",

"Set a **retention period** for personal data used in development (don’t just keep training data forever) [56] . The guidance advises deciding upfront how long data (and models with personal data) will be kept (Step 6).",
        "Always perform a **DPIA** for high-risk AI (very likely required for most AI involving personal data, per CNIL’s criteria) [58] . Integrate privacy by design controls (Step 7) and document all choices."
      ],
      "questions": [
        "Has the AI project defined a clear, specific purpose for personal data use, and is the data being collected strictly necessary for that purpose (avoiding use of irrelevant or excessive data)?",
        "Has the organization determined and documented the lawful basis for each phase of the AI data processing (e.g. separate bases for model training vs. end-user predictions), and if relying on legitimate interest, conducted and recorded a proper balancing test?",

"If personal data collected for one purpose is being reused to train the AI, has the organization checked for purpose compatibility or obtained fresh consent
```

```
where needed to prevent unlawful secondary use?",
        "Did the project establish data retention limits for personal data (and
model outputs containing personal data), and are there processes to delete or
anonymize data once no longer needed for the stated purpose?",
        "Was a Data Protection Impact Assessment conducted before deploying the
AI system, and were data protection measures (privacy by design) built in – for
example, techniques to minimize personal data exposure or mechanisms to enable
data subject rights?"
      ],
      "expected_answers": [
        {
          "question": "Has the AI project defined a clear, specific purpose for
personal data use, and is the data being collected strictly necessary for that
purpose (avoiding use of irrelevant or excessive data)?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(b)", "5(1)(c)"],
          "rationale": [
            "CNIL's guidance insists on purpose specification to enable data
minimization. If the project has an explicit purpose statement (e.g. "predictive
maintenance on X using personal data Y") and only collects data relevant to
that, it meets these requirements.",
            "Auditors would expect to see documentation of the AI's purpose and
a rationale for each data category used. If this exists and no extraneous
personal data is found in the training set, that indicates compliance with Art.
5(1)(b)&(c).",
            "Clear purpose definition and necessity filtering of data would
result in no violation signals – the project is adhering to GDPR's foundational
principles."
          ]
        },
        {
          "question":
"Has the organization determined and documented the lawful basis for each phase
of the AI data processing (e.g. separate bases for model training vs. end-user
predictions), and if relying on legitimate interest, conducted and recorded a
proper balancing test?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["6", "5(2)"],
          "rationale": [
            "The guidance (echoing ICO and others) says to split AI development
vs deployment and select appropriate legal bases for each 8 72 . If the
organization has a GDPR-compliance file showing, for example, that training data
is processed under legitimate interests (with a completed LIA), and user-facing
decisions under contract necessity or consent, this is a good sign.",
            "Proper documentation (accountability Art.5(2)) of the lawful basis
decisions, especially a legitimate interest assessment if used, would fulfill
```

```
GDPR expectations. The absence of such documentation would be a red flag.",
            "Assuming the organization followed CNIL's Step 3 and has this
clearly in place, the audit would find no violation signal here."
          ]
        },
        {
          "question": "If personal data collected for one purpose is being
reused to train the AI, has the organization checked for purpose compatibility
or obtained fresh consent where needed to prevent unlawful secondary use?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["PURPOSE_CREEP"],
          "gdpr_refs": ["5(1)(b)", "6(4)"],
          "rationale": [
            "Step 4 of CNIL's recommendations covers re-use of data [54]. If the
AI project is feeding on data that was originally gathered for a different
purpose, GDPR Article 6(4) requires a compatibility assessment (or new
consent).",
            "This is a common grey area – e.g., using customer support data to
train an unrelated AI tool. Auditors would need to see evidence of a
compatibility analysis. If none is provided, it's a potential violation (purpose
limitation).",
            "Therefore, this question would need careful review. If the
organization cannot demonstrate it addressed this, a 'purpose creep' signal is
warranted. If they did (e.g., documented that training is compatible with
original purpose, or re-collected consent), then it would pass."
          ]
        },
        {
          "question": "Did the project establish data retention limits for
personal data (and model outputs containing personal data), and are there
processes to delete or anonymize data once no longer needed for the stated
purpose?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(e)"],
          "rationale": [
            "CNIL's Step 6 presses for setting a retention period during AI
development [56]. If the team defined, say, "we will keep training datasets with
personal data for X months then purge or anonymize," that's compliant with
storage limitation.",
            "Auditors would verify if data and intermediate results aren't kept
indefinitely. If procedures (like periodic deletion scripts or policies) exist
and were followed, that's a pass – no excessive retention signal.",
            "If the project can show it only retains data as long as necessary
(and perhaps implements pseudonymization or aggregation after training), it
aligns with GDPR's retention principle."
          ]
        },
```

```
        {
          "question": "Was a Data Protection Impact Assessment conducted before
deploying the AI system, and were data protection measures (privacy by design)
built in – for example, techniques to minimize personal data exposure or
mechanisms to enable data subject rights?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["35", "25"],
          "rationale": [
            "For most AI processing personal data, a DPIA is mandatory (high
risk likely). CNIL (and EDPB) require it be done prior to go-live. If the
organization did a DPIA identifying risks (bias, re-identification, etc.) and
addressing them, that's a strong compliance indicator.",
            "Privacy by design measures might include using synthetic data,
anonymizing inputs, or allowing users to opt-out – all of which CNIL encourages.
Evidence of such measures (like documented use of anonymization techniques,
differential privacy, etc.) shows compliance with Art.25.",
            "If these steps were demonstrably taken, the AI system meets GDPR's
accountability and risk mitigation expectations. No signals of violation would
be recorded on these points."
          ]
        }
      ],
      "ambiguity_notes": "This guidance is non-binding but reflects CNIL's
expectations. One subtle area is legal basis for AI training – CNIL suggests it
*can* be legitimate interest, but that requires careful balancing. Compatibility
of reuse (Art.6(4)) is another nuanced area – knowing when you need new consent
for training data is context-dependent. Overall, the guidance translates GDPR to
AI with principles, but controllers still face interpretative questions (e.g.,
how to practically apply data minimization in large-scale AI and when a DPIA is
required – likely almost always for AI, but not explicitly mandated in all
cases)."
    },
    {
      "id": "gs_007",
      "title": "ICO (UK) – Guidance on AI and Data Protection (Auditing
Framework)",
      "authority": "UK Information Commissioner's Office",
      "jurisdiction": "United Kingdom (UK GDPR)",
      "date": "30 July 2020 (initial publication; updated 2021-2023)",
      "source_url": "https://ico.org.uk/for-organisations/guide-to-data-
protection/key-data-protection-themes/guidance-on-ai-and-data-protection/",
      "excerpt":
"Whenever you are processing personal data – whether to train a new AI system,
or make predictions using an existing one – you must have an appropriate lawful
basis to do so. Different lawful bases may apply depending on your particular
circumstances... Remember that it is your responsibility to decide which lawful
basis applies to your processing; you must always choose the basis that most
```

```
closely reflects the true nature of your relationship with the individual and the purpose of the processing, and you should document your decision. You cannot swap lawful bases at a later date without good reason. You must include your lawful basis in your privacy notice, and if processing special category data you need both a lawful basis and an additional condition [8].",
      "ai_relevance_tags": ["accountability", "lawful_basis", "transparency", "fairness", "accuracy", "security", "DSR_access", "automated_decision"],
      "facts_summary": [
        "The ICO's guidance (part of its AI Auditing Framework) provides best practices and ICO's interpretation of how UK GDPR applies to AI systems. It covers governance and accountability, transparency to data subjects, lawfulness, fairness (including bias/discrimination), accuracy, data minimization and security, and individual rights in AI [70] [65].",
        "Accountability: Organizations should document their AI system's design and decisions thoroughly (e.g. DPIAs, algorithmic impact assessments). They need to be able to demonstrate compliance for each aspect (privacy by design).",
        "Transparency: Controllers should tell individuals when AI is used and how. The ICO references its separate guidance *Explaining decisions made with AI* for how to provide meaningful explanations.",

"Lawfulness: Choose a lawful basis for each processing step (training vs inference) and record it. The guidance emphasizes not to repurpose legal bases arbitrarily [9]. If special category data is involved (e.g. inferring health data), make sure an Art.9 condition is also in place.",
        "Fairness: The ICO calls for bias monitoring and mitigation. AI should not result in unjust outcomes or discrimination. If Article 22 (automated decisions with legal/significant effects) applies, ensure an exception applies and that **human review** and **explanation** are provided [85].",
        "Accuracy: Organizations must address AI outputs that may be incorrect. Statistical accuracy and data accuracy both matter – e.g., preventing false personal data. The guidance suggests measures to ensure data used is accurate and up to date.",
        "Security and minimization: Implement appropriate technical measures (the framework suggests techniques like pseudonymization, encryption for training data). Only use data actually needed – avoid large dumps of data "just in case".",
        "Individual rights: Even if AI is complex, individuals retain rights like access (including getting "meaningful information about logic" under Art. 15) and erasure. Controllers should have processes to extract an individual's data from models or at least suppress outputs related to them."
      ],
      "questions": [
        "Has the organization documented the lawful basis for all personal data processing in the AI lifecycle (and, where applicable, a special category condition), and is this reflected in the privacy notice?",
        "Does the organization ensure transparency to individuals about AI usage, providing clear information about how their data is used and how decisions are made (including the existence of automated decision-making and
```

```
meaningful information about logic)?",
        "What measures are in place to monitor and ensure the fairness of AI
outcomes (e.g. avoiding discriminatory impacts), and if the AI makes solely
automated decisions with legal or similarly significant effects, are individuals
informed and given the right to human review?",
        "How does the organization ensure the accuracy of personal data used in
training and the accuracy of AI outputs relating to individuals? If the AI can
produce incorrect personal information, are there processes to correct or
mitigate this?",
        "Has the organization implemented data minimization and security
controls in the AI system (e.g. using only necessary training data, anonymizing
or pseudonymizing data, protecting training and model data against breaches)?",

"Can individuals exercise their GDPR rights in relation to the AI system
(access, rectification, erasure, objection)? For example, can a person get an
explanation of a decision affecting them or request their data be removed from
the model's training set?"
      ],
      "expected_answers": [
        {
          "question": "Has the organization documented the lawful basis for all
personal data processing in the AI lifecycle (and, where applicable, a special
category condition), and is this reflected in the privacy notice?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["6", "9", "13"],
          "rationale": [
            "The ICO expects explicit documentation of lawful bases [9]. An
organization following this guidance would have, for example, records that
"training phase – lawful basis: legitimate interests (LIA completed); deployment
phase – lawful basis: consent (obtained via app)".",
            "If such documentation exists and the public privacy notice also
states the bases (as required by Art.13/14), the organization is in compliance.
There's no sign of violation if lawful basis choices are made and disclosed
properly.",

"Absence of documented lawful bases would be a concern, but assuming the best-
case (they followed ICO's guidance), this is marked as PASS with no violation
signals."
          ]
        },
        {
          "question": "Does the organization ensure transparency to individuals
about AI usage, providing clear information about how their data is used and how
decisions are made (including the existence of automated decision-making and
meaningful information about logic)?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
```

```
          "gdpr_refs": ["13", "15", "22"],
          "rationale": [
            "The ICO guidance stresses transparency and refers to its AI
explainability guidance [62]. A compliant organization will have updated privacy
notices explaining AI processing, and if automated decisions are made, they
inform users of their rights and some logic overview.",
            "For instance, a bank using AI for credit decisions should tell
applicants that an algorithm evaluates them and list the main factors. The
presence of such disclosures (and internal documentation on how to explain
decisions) indicates compliance.",

"If auditors find evidence of user-facing explainability (simplified logic info,
reasons provided for decisions, etc.), then transparency obligations under Art.
13, 15 and 22(3) are being met. Thus no transparency violation signal."
          ]
        },
        {
          "question": "What measures are in place to monitor and ensure the
fairness of AI outcomes (e.g. avoiding discriminatory impacts), and if the AI
makes solely automated decisions with legal or similarly significant effects,
are individuals informed and given the right to human review?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["BIAS_RISK", "NO_HUMAN_INTERVENTION"],
          "gdpr_refs": ["5(1)(a)", "22"],
          "rationale": [
            "Fairness is a nuanced principle. The ICO guidance calls for
assessing AI for bias and discrimination. Auditors would need to see if the
organization has fairness metrics or bias audits. If none exist, that’s a
concern (potential indirect discrimination, violating Art.5(1)(a) fairness).",
            "If the AI is used for significant decisions (hiring, credit
approval) with no human involvement, Article 22 triggers. The ICO is clear that
individuals then must have a way to obtain human review and not be simply
subjected to the algorithm. Lack of such a mechanism would be a violation.",

"This area often requires careful review. The answer would depend on evidence:
e.g., if logs of bias testing or an option for users to contest decisions exist.
If not, signals like “bias risk” or “no human intervention” would be flagged.
It’s marked NEEDS_REVIEW to reflect that auditors must examine fairness controls
in detail."
          ]
        },
        {
          "question":
"How does the organization ensure the accuracy of personal data used in training
and the accuracy of AI outputs relating to individuals? If the AI can produce
incorrect personal information, are there processes to correct or mitigate
this?",
          "expected_verdict": "NEEDS_REVIEW",
```

```
          "expected_violation_signals": ["DATA_ACCURACY_ISSUES"],
          "gdpr_refs": ["5(1)(d)"],
          "rationale": [

"Data accuracy (Art.5(1)(d)) is challenging for AI. The ICO guidance discusses
accuracy in both input data and model predictions. Auditors will look for steps
like: cleaning training data, removing known errors, and handling output errors
(e.g., if the AI associates wrong info to a person).",
            "If the AI has a propensity to “hallucinate” or mix data, the
organization should have mitigation (perhaps not outputting data about
individuals or having humans validate critical outputs). If no such measures
exist, it’s a potential violation of the accuracy principle.",
            "This is case-specific. Thus, NEEDS_REVIEW: The auditor might need
to test the system’s outputs or review incident logs. Any pattern of inaccurate
personal data being generated without correction would raise a “data accuracy”
violation signal."
          ]
        },
        {
          "question": "Has the organization implemented data minimization and
security controls in the AI system (e.g. using only necessary training data,
anonymizing or pseudonymizing data, protecting training and model data against
breaches)?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(c)", "32"],
          "rationale": [
            "The ICO guidance aligns with GDPR principles of minimization and
security. If the project followed best practices (e.g., did not scoop up
extraneous personal data, perhaps used synthetic data where possible, and
secured its datasets), auditors would find documentation of that.",
            "For example, using pseudonymized IDs in place of names during
training, encrypting the training database, and access controls for the model
would all be positive indicators of compliance with Art.32 and Art.5(1)(c).",
            "Assuming the organization can demonstrate these controls (via
technical architecture documents, DPIA, etc.), it would be a pass – no signals
triggered in these areas."
          ]
        },
        {
          "question":
"Can individuals exercise their GDPR rights in relation to the AI system
(access, rectification, erasure, objection)? For example, can a person get an
explanation of a decision affecting them or request their data be removed from
the model’s training set?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["DSR_OBSTRUCTION"],
          "gdpr_refs": ["15", "16", "17", "21", "22"],
```

```
          "rationale": [
            "Enabling data subject rights with AI can be complex. The ICO expects organizations to figure it out – e.g., provide Article 15 information including logic (the “meaningful information” about the algorithm), and handle erasure requests even for training data if feasible.",
            "Auditors would check if, for instance, the company has a procedure for someone to ask “What data of mine was used by the AI?” or “Please delete me from the training set.” If the answer is “we can’t because it’s mixed into the model,” that’s problematic without at least an attempt at accommodation.",
            "This likely needs review. If the company has a portal or process for AI-related requests (as some do, allowing opt-outs from training), that mitigates issues. If it has nothing, then a DSR compliance signal is raised. The verdict depends on evidence of how rights are handled in practice."
          ]
        }
      ],
      "ambiguity_notes": "The ICO’s guidance is broad and non-binding. UK GDPR overlaps EU GDPR but has minor differences (e.g., no Art.22 equivalent in exact words, though UK law is similar). One ambiguity is how to provide “meaningful information” about AI logic – organizations struggle with how much to reveal without infringing IP or complexity barriers. Also, the guidance suggests best practices (like bias auditing) not explicitly in GDPR law – failure to do them isn’t a direct violation per se, but could lead to indirect violations of fairness or accuracy. Thus, auditors must interpret absence of such practices in context."
    },
    {
      "id": "gs_008",
      "title": "NL Court (Amsterdam) – Drivers vs. Uber & Ola (Algorithmic Management)",
      "authority": "Amsterdam District Court (Netherlands)",
      "jurisdiction": "Netherlands (EU)",
      "date": "11 March 2021 (first instance judgments)",
      "source_url": "http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html",
      "excerpt": "In one case (Ola), the Court required the company to explain the logic behind a fully automated decision (penalties and deductions system) to the drivers, recognizing for the first time a right to an explanation under the GDPR. The Court stated that \"Ola must communicate the main assessment criteria and their role in the automated decision to the drivers, so that they can understand the criteria on the basis of which the decisions were taken and are able to check the correctness and lawfulness of the processing\". In another case (Uber), the Court found that certain algorithmic management decisions did not qualify as “solely automated” because humans were involved, so Article 22 GDPR was not triggered.",
      "ai_relevance_tags": ["automated_decision", "profiling", "DSR_access", "transparency", "fairness"],
      "facts_summary": [
```

```
        "This set of cases was brought by ride-hailing drivers who challenged the lack of transparency in Uber's and Ola's algorithmic management (e.g. automated terminations, payment deductions). They invoked GDPR rights to access data and information about automated decisions (Articles 15 and 22).",
        "The Court ruled that **Article 22 GDPR can create a "right to an explanation."** In the Ola case, a system that automatically issued monetary penalties to drivers for alleged irregularities was found to "significantly affect" them. Ola was ordered to provide drivers with the *meaningful information about the logic* of those automated decisions [77] [74].",
        "For other aspects (like Uber's order dispatch algorithm and account deactivations for alleged fraud), the Court found either that they did not meet the threshold of "legal or similarly significant effect" or were not purely automated (because Uber had human review teams in the loop) [76]. Thus, in those instances, Article 22 did not apply and the drivers' demands for algorithmic logic were partly rejected.",
        "However, the Court did enforce GDPR's transparency and access provisions: Uber had to disclose certain personal data and ratings about drivers (Article 15) and could not simply refuse on trade secret grounds. It also emphasized that **imbalance of power** (gig workers vs platform) reinforced the need for GDPR's protections.",
        "In sum, the judgments affirm drivers' rights to algorithmic transparency where fully automated, impactful decisions occur, marking one of the first judicial recognitions of a GDPR-based right to explanation."
      ],
      "questions": [
        "If the platform issues automated decisions that significantly affect a worker (like automatic fines or account suspensions), does it provide the worker with meaningful information about the logic and criteria used, as required by GDPR?",
        "Are there human oversight or review mechanisms for important decisions (e.g. account deactivation for suspected fraud), or are decisions solely made by algorithms without human involvement?",
        "When drivers request access to their data and information on algorithmic decisions (under Art.15), does the company provide it (including factors and scores), or is it withholding such information improperly (e.g. citing trade secrets too broadly)?"
      ],
      "expected_answers": [
        {
          "question": "If the platform issues automated decisions that significantly affect a worker (like automatic fines or account suspensions), does it provide the worker with meaningful information about the logic and criteria used, as required by GDPR?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_EXPLANATION_PROVIDED"],
          "gdpr_refs": ["22", "15"],
          "rationale": [
            "The Dutch court held that in Ola's case, the lack of explanation
```

```
for automated penalty decisions was not compliant. GDPR implicitly requires
meaningful information about automated decision logic (via Art.15 and 22).",
            "If the platform did not already give such information, that's a
violation of transparency rights. The court compelled Ola to communicate the
main criteria and their role in the algorithm – indicating prior omission was a
breach.",
            "Therefore, absent evidence that the company proactively provides
algorithmic explanations for impactful automated decisions, we flag a failure to
comply with GDPR's requirement (as interpreted by this case)."
          ]
        },
        {
          "question": "Are there human oversight or review mechanisms for
important decisions (e.g. account deactivation for suspected fraud), or are
decisions solely made by algorithms without human involvement?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["SOLELY_AUTOMATED_DECISION"],
          "gdpr_refs": ["22"],
          "rationale": [
            "Article 22 prohibits solely automated decisions with significant
effects unless an exception applies and appropriate safeguards (like human
review) are in place. The court drew a line: Uber's fraud deactivations had some
human involvement, so they escaped Art.22 [76] .",
            "If an audit finds any fully automated firing/suspension without
human checks, that would be non-compliant (unless consent or contract necessity
can be invoked, which is unlikely in gig work). It *needs review* because we
must verify the actual process.",
            "In practice, companies often claim humans "review" such decisions.
We'd examine if that's true or a token gesture. A genuine human-in-the-loop
would mitigate the violation; if it's solely automated in reality, it triggers
an Art.22 issue."
          ]
        },
        {
          "question":
"When drivers request access to their data and information on algorithmic
decisions (under Art.15), does the company provide it (including factors and
scores), or is it withholding such information improperly (e.g. citing trade
secrets too broadly)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["DSR_ACCESS_DENIED"],
          "gdpr_refs": ["15", "20"],
          "rationale": [

"In these cases, drivers had to litigate to get their data. Uber/Ola initially
resisted giving full information (likely citing IP/confidentiality), but the
court ordered disclosure of key data points and logic under Art.15.",
```

```
"If the platform was previously denying or only partially fulfilling access requests about algorithm data, that's a GDPR violation. Trade secrets are not absolute; Recital 63 says they can't justify refusing all info.",
            "Thus, unless the company has changed practices post-judgment, this aspect was a fail. The drivers' win indicates the companies weren't fully compliant with access rights – now they are expected to improve transparency in response to DSARs."
          ]
        }
      ],
      "ambiguity_notes": "These rulings were pioneering. They interpret GDPR as giving a de facto right to explanation, but this isn't explicitly in the text – it's derived from Articles 15 and 22. There's ambiguity in when an automated decision is "similarly significant" (the judges found Ola's fines were, but Uber's matching wasn't). Also, what constitutes "meaningful information" about an algorithm remains open – the court required main criteria, but not the entire source code. Lastly, since this is a lower court decision, it sets persuasive but not binding precedent beyond the Netherlands; interpretation may evolve as higher courts or other jurisdictions weigh in."
    },
    {
      "id": "gs_009",
      "title": "CJEU – Österreichische Post (UI) Case on Inferred Political Opinions",
      "authority": "Court of Justice of the EU (CJEU)",
      "jurisdiction": "EU (Austria)",
      "date": "4 May 2023 (Judgment in Case C-300/21)",
      "source_url": "https://curia.europa.eu/juris/document/document.jsf?docid=271053",
      "excerpt": "Österreichische Post had generated information on the political affinities of individuals using an algorithm that considered various data (e.g. demographics). The CJEU confirmed that even inferred data can fall under special categories if it reveals sensitive information about a person. It noted that assigning someone a high probability of affinity to a political party constitutes processing of data \"revealing political opinions\" within the meaning of Article 9(1) GDPR [80]. Such processing, done without a valid Article 9(2) exception (and without the person's consent), was unlawful. The Court also ruled on damages, holding that a mere GDPR violation does not automatically entitle compensation absent actual harm.",
      "ai_relevance_tags": ["profiling", "special_category", "inference", "lawful_basis", "damages"],
      "facts_summary": [
        "Austria's postal service (Post AG) profiled citizens for marketing: it statistically inferred political party affinities for millions of Austrians based on characteristics like address and demographics [80]. It then sold this data to advertisers (political and commercial). The plaintiff discovered he was profiled as having a high affinity for a certain political party, which he found offensive.",
```

```
"No consent was obtained for this profiling; Post AG argued it was using publicly available data and its own algorithm under legitimate interest. It provided minimal notice of this processing.",
        "The plaintiff sued, seeking deletion of the inferred data (which the Post agreed to) and €1,000 in non-material damages for distress. Austrian courts asked the CJEU to clarify two points: (1) Does inferring someone’s political leanings count as processing special category data under Article 9 GDPR? (2) Is compensation under Article 82 GDPR available even without tangible harm (is a mere violation enough for damages)?",

"On (1), **the CJEU held yes**: inferring sensitive traits is processing of sensitive data. Even if the data input isn’t sensitive, the output “reveals” a political opinion (albeit probabilistic) and thus triggers Article 9’s higher protections. This implies data controllers cannot evade Article 9 by saying “it’s only a prediction.”",
        "On (2), the CJEU said a GDPR breach alone doesn’t automatically merit compensation; some harm must be shown, but it set a low bar by rejecting any de minimis threshold for damage. In short, every violation of GDPR must be compensable if it causes the person more than trivial upset – but a mere breach without any effect might not result in damages.",
        "The Post case highlighted that using algorithms to infer protected characteristics (politics, health, etc.) without explicit consent or other Art. 9(2) grounds is unlawful. Austrian Post had to stop this and faced national penalties and lawsuits (though the CJEU aspect was primarily about damages)."
      ],
      "questions": [
        "Does the AI’s profiling infer any special category data about individuals (such as political opinions or health status)? If so, has the controller obtained explicit consent or another Article 9(2) exception for processing that inferred sensitive data?",
        "If the system generates or uses such sensitive inferences without consent, is this processing recognized and handled as special category data (with appropriate safeguards)? Or is the controller incorrectly treating these inferences as non-sensitive data?",
        "In case of unlawful profiling, what is the potential liability? (E.g., could individuals claim compensation for non-material harm if they discover the AI has profiled them in a sensitive or offensive way without their consent?)"
      ],
      "expected_answers": [
        {
          "question": "Does the AI’s profiling infer any special category data about individuals (such as political opinions or health status)? If so, has the controller obtained explicit consent or another Article 9(2) exception for processing that inferred sensitive data?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["SPECIAL_DATA_NO_CONDITION"],
          "gdpr_refs": ["9"],
```

```
          "rationale": [
            "The CJEU made clear that inferring a likely political preference =
processing special category data. So if the AI profiles people into sensitive
categories without Art.9(2) basis, it's unlawful.",
            "In our audit, if we find the system is deriving, say, health
predictions or ethnic proxies or political leanings from data, and the company
did not realize this triggers Article 9, it likely has no consent or other
exemption in place – a serious violation.",
            "Thus, absent evidence of an explicit consent for those inferences,
we mark this as FAIL. The CJEU decision affirms that controllers must treat such
inferred attributes with the same strictness as provided data."
          ]
        },
        {
          "question":
"If the system generates or uses such sensitive inferences without consent, is
this processing recognized and handled as special category data (with
appropriate safeguards)? Or is the controller incorrectly treating these
inferences as non-sensitive data?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["MISCLASSIFIED_SENSITIVE_DATA"],
          "gdpr_refs": ["9", "5(1)(a)"],
          "rationale": [
            "Following the Austrian Post scenario, the issue was the controller
did *not* treat the political affinity data as sensitive. It assumed it could
profile under legitimate interest, which was wrong [80] .",
            "If our audited organization similarly misclassifies sensitive
inferences as ordinary data, it means they're missing required safeguards (like
consent or an Article 9(2) condition and higher protection measures). That's a
compliance failure.",

"We'd likely find that no DPIA considered Article 9 implications, no consent
obtained. This signal indicates the controller's internal compliance framework
failed to flag and properly handle special category data derived by the AI."
          ]
        },
        {
          "question": "In case of unlawful profiling, what is the potential
liability? (E.g., could individuals claim compensation for non-material harm if
they discover the AI has profiled them in a sensitive or offensive way without
their consent?)",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["POTENTIAL_COMPENSATION_RISK"],
          "gdpr_refs": ["82"],
          "rationale": [
            "The CJEU in UI v Österreichische Post clarified that individuals
can claim compensation for GDPR breaches, but they must show some form of harm
(even if just emotional distress).",
```

```
            "If an AI unlawfully profiles someone (e.g., labels them as likely having a certain political leaning or illness) and they find out, they might claim that caused them distress or reputational harm. Under GDPR Article 82, they could seek monetary compensation.",

"This is a risk area rather than a binary compliance yes/no. We flag it as NEEDS_REVIEW: the organization should be aware that such breaches could lead to class actions or individual claims. It’s not a direct “violation signal” of GDPR obligations, but it is a legal risk stemming from the violation. Therefore, auditors note this as a serious consequence to review with legal counsel."
          ]
        }
      ],
      "ambiguity_notes": "This CJEU ruling settled some debate by saying inferred data can be sensitive, aligning with WP29’s stance [1]. But it raises practical ambiguities: how certain or explicit must an inference be to count as Article 9 data? (The Court didn’t require 100% certainty; a probability was enough.) Controllers now have to err on the side of caution. Also, on damages, while the Court rejected a 'de minimis' threshold, it left open what qualifies as actionable harm – that will be decided by national courts case by case. Organizations should assume that if people are upset or feel exposed by AI’s profiling, they might claim compensation, even if the harm is intangible."
    },
    {
      "id": "gs_010",
      "title": "EDPB Guidelines on Virtual Voice Assistants (VVAs)",
      "authority": "European Data Protection Board",
      "jurisdiction": "EU",
      "date": "7 July 2021 (final version)",
      "source_url": "https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en",
      "excerpt": "Some VVA services retain personal data until users request deletion. This is not in line with the storage limitation principle. **VVAs should store data for no longer than is necessary** for the purposes [57]. The guidelines identify common purposes for VVAs: executing user requests (which can be done without consent, as it’s necessary for the service), improving the ML model, biometric identification, and profiling for ads. For any purposes beyond the user’s request, **prior consent is required** (e.g. using voice data to improve the model or for personalized advertising triggers ePrivacy and GDPR consent) and data minimization must be observed. It also recommends privacy-by-design measures like on-device processing and immediate deletion of raw audio when possible.",
      "ai_relevance_tags": ["voice_assistant", "special_category", "biometrics", "data_retention", "lawful_basis", "consent", "privacy_by_design"],
      "facts_summary": [

"EDPB’s VVA guidelines focus on smart assistants (like Siri, Alexa) that use AI to process voice commands. These involve continuous listening, speech-to-text
```

```
AI, and often sending audio to cloud servers – raising privacy concerns.",
        "Key guidance points: **Transparency & consent:** When setting up a
voice assistant, users must be informed (Art.13). If the assistant will use
voice data for anything beyond executing the user's request (like training ML
models or targeted ads), that likely requires opt-in consent (especially due to
ePrivacy rules for voice data storage).",
        "**Storage limitation:** VVAs should not keep voice recordings or
transcripts indefinitely. The EDPB criticized that some assistants kept data
until deletion request, which violates Art.5(1)(e) [57]. Data (especially raw
audio) should be deleted or anonymized once no longer needed for the stated
purpose.",
        "**Special data:** Voices can be biometric data (if used to identify a
person's identity) – requiring explicit consent under GDPR Art.9 unless another
exception applies. If a VVA has a voice recognition feature to recognize the
user, that's processing special category biometric data and must meet Art.9
conditions (usually explicit consent).",
        "Children's voices: extra caution since kids may use assistants –
parental consent and age-appropriate measures are necessary (not explicitly in
excerpt but in broader guidelines).",
        "Privacy by design: The guidelines encourage local processing (not
sending everything to cloud), allowing users to use the service without
extensive personal data collection, and offering settings (like opt-out of data
retention or human review of recordings).",
        "Security: VVAs often sit in homes always listening – data must be
encrypted, stored safely, and robustly secured given sensitivity (conversations
can be very private). Also, accidental activation and recording of non-command
speech is a risk; EDPB says mitigate that (like voice activation algorithms
should be tuned to avoid false activations)."
      ],
      "questions": [
        "Does the voice assistant service automatically delete or anonymize
voice recordings and transcripts after fulfilling the user's request, or is it
retaining data indefinitely until the user manually deletes it?",

"If the assistant uses voice data for secondary purposes (like improving its
speech recognition AI or for personalized services), is it obtaining users'
consent for those purposes, as required by GDPR (and ePrivacy)?",

"Are there measures to minimize data collection (for example, processing
commands locally, not recording background audio, and not collecting more data
than necessary for the spoken request)?",
        "If the assistant features voice profile recognition (identifying the
speaker), is that treated as biometric data processing with explicit consent and
proper safeguards? Similarly, are users informed and consenting if their voice
commands are being used to personalize ads or content (profiling)?"
      ],
      "expected_answers": [
        {
```

```
          "question": "Does the voice assistant service automatically delete or
anonymize voice recordings and transcripts after fulfilling the user's request,
or is it retaining data indefinitely until the user manually deletes it?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["UNLIMITED_RETENTION"],
          "gdpr_refs": ["5(1)(e)"],
          "rationale": [
            "The EDPB explicitly says retaining voice data until user deletion
is non-compliant [57]. If our audit finds the VVA keeps all voice recordings
forever by default, that's a clear storage limitation breach.",

"Unless the service has implemented automatic deletion (e.g., delete audio after
a few minutes or once processed) or at least a short retention period, it fails
Art.5(1)(e). Many early VVAs did keep data indefinitely for ML training; this
guideline says that's not acceptable.",
            "Therefore, if indefinite retention is in place, we mark FAIL. The
service should be designed to purge data once it's no longer needed for the
immediate purpose."
          ]
        },
        {
          "question": "If the assistant uses voice data for secondary purposes
(like improving its speech recognition AI or for personalized services), is it
obtaining users' consent for those purposes, as required by GDPR (and
ePrivacy)?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["MISSING_CONSENT_SECONDARY_USE"],
          "gdpr_refs": ["6(1)(a)", "9(2)(a)", "5(3) ePrivacy Dir"],
          "rationale": [

"Executing a user's command may be lawful under contract necessity – but using
the voice data to improve the ML model or to profile the user for ads is a
different purpose. The guidelines indicate those require consent.",
            "We need to review what the service does. If it by default sends
audio snippets for model training or analytics without separate consent, that's
a violation of both GDPR (different purpose needs separate basis) and ePrivacy
(storing/accessing info on user device needs consent unless strictly
necessary).",
            "If the service has an opt-in toggle like "Help Improve our service
by sharing your recordings", and only uses data when consent given, then it's
fine. Without that, this is a likely violation signal. It's marked NEEDS_REVIEW
as we must examine the specific data flows and user agreements."
          ]
        },
        {
          "question": "Are there measures to minimize data collection (for
example, processing commands locally, not recording background audio, and not
collecting more data than necessary for the spoken request)?",
```

```
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["5(1)(c)", "25"],
          "rationale": [
            "If the service follows recommendations, it will implement some on-
device processing (e.g., wake-word detection locally, so it doesn't send
everything said in the room to the cloud). It will also only listen after
activation and stop shortly after fulfilling the request.",
            "Auditing technical architecture: If we see that the system isn't
constantly streaming audio, and it filters out background noise, etc., then data
minimization is respected. Privacy by design (Art.25) is demonstrated through
these controls.",
            "Assuming the product has matured to incorporate these privacy
features (many have after public pressure), we give a PASS. There are no
violation signals if the assistant truly limits data capture to what's needed
for user interaction."
          ]
        },
        {
          "question": "If the assistant features voice profile recognition
(identifying the speaker), is that treated as biometric data processing with
explicit consent and proper safeguards? Similarly, are users informed and
consenting if their voice commands are being used to personalize ads or content
(profiling)?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["BIOMETRIC_NO_CONSENT",
"PROFILING_NO_CONSENT"],
          "gdpr_refs": ["9", "6(1)(a)", "22"],
          "rationale": [
            "Voice ID is biometric identification. GDPR requires explicit
consent or another Art.9 exception for that. If the VVA just enrolls voice
profiles by default to distinguish users without explicit opt-in, that's
problematic.",
            "Likewise, using voice interaction data to build a profile on the
user's preferences (for ads, etc.) triggers profiling/automated decision rules –
likely needing consent and certainly transparency.",
            "This area requires inspection of settings: Does the setup flow ask
"Do you want voice recognition enabled?" with consent? Is there a clear notice
about personalized ads? We mark NEEDS_REVIEW. If such features are on by default
with no consent, it's a violation (signals: Biometric without consent, Profiling
consent missing). If the features are off until opted-in, then it's okay."
          ]
        }
      ],
      "ambiguity_notes": "These guidelines combine GDPR and ePrivacy aspects.
One challenge is distinguishing what's "strictly necessary" for providing the
service (no consent needed under ePrivacy) versus what counts as additional
processing requiring consent. EDPB draws the line that anything beyond executing
```

```
a user’s command (like improving the AI itself) needs consent – but some might argue legitimate interest for improvement. Regulators clearly lean toward consent. Another ambiguity: voice data often contains incidental personal data of others (background voices) – the guidelines urge filtering that out, but technically that’s hard. Compliance in practice may vary. Lastly, defining a retention period for voice data (how long is “necessary”) is somewhat case-by-case – but indefinite retention is plainly disapproved."
    },
    {
      "id": "gs_011",
      "title": "Italian Garante – Foodinho/Glovo Algorithmic Management Fine",
      "authority": "Garante (Italian Data Protection Authority)",
      "jurisdiction": "Italy",
      "date": "5 July 2021",
      "source_url": "https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9675440",
      "excerpt": "The Italian SA found that Foodinho (Glovo) had failed to adequately inform its rider employees about the functioning of the algorithms used for order distribution and performance rating, and it had not implemented measures to ensure the accuracy and fairness of algorithmic outcomes. It also lacked procedures for riders to obtain human intervention or contest automated decisions (like exclusion from work assignments). The Garante fined Foodinho €2.6 million and ordered it to **check the accuracy and relevance of all data used by the system** (e.g. GPS tracks, delivery times, customer ratings) to minimize errors and biases that could reduce riders’ work opportunities [11].",
      "ai_relevance_tags": ["automated_decision", "employment", "transparency", "accuracy", "fairness", "DSR_objection"],
      "facts_summary": [
        "Foodinho, a subsidiary of Glovo, uses algorithms (“Frank” for order dispatching, “Jarvis” for shift planning) to manage its gig delivery riders. After investigation, the Garante found multiple GDPR and labor law violations in how this algorithmic management operated [11].",
        "**Transparency failure:** Riders were given almost no information on how the algorithm assigned orders or evaluated them. This violates Art.13 (employees should be informed about automated decision logic affecting them).",
        "**Accuracy & bias:** The algorithm took into account various data (GPS location, completed orders, customer feedback, acceptance rates) but Foodinho had no safeguards to ensure this data was correct or to prevent unfair biases (e.g., a rider could be penalized for GPS errors or customer prejudices). The DPA demanded Foodinho verify and improve data quality.",
        "**No human intervention/right to contest:** Decisions like reducing a rider’s priority or blocking them from the platform were made automatically. Foodinho had no clear procedure for riders to request human review or appeal these decisions – violating Art.22(3). Riders essentially had no say, contrary to GDPR and new Italian labor rules.",

"Excessive data: The system tracked and stored detailed data (continuous geolocation pings every 15 seconds, etc.) on ~19,000 riders. The DPA noted this
```

```
as intrusive and ordered minimization.",
        "Outcome: Fine of €2.6M and an order for Foodinho to fix issues within
60 days. It had to implement transparency (algorithm info in privacy notices,
rider communications), allow human oversight on decisions, audit and correct
data and bias in the algorithms, and involve its DPO and workers in algorithm
assessments going forward."
      ],
      "questions": [
        "Are riders provided with clear information about the algorithmic
systems that assign orders and evaluate performance, including the main
parameters and criteria used?",
        "Has the company implemented measures to ensure that data feeding the
algorithm (GPS data, delivery times, customer ratings, etc.) is accurate and
that any errors or biases (e.g. unfair negative ratings) do not unduly affect
riders' scores?",

"If the algorithm reduces a rider's job opportunities (e.g. fewer orders or
shifts) or deactivates them, is there a mechanism for the rider to request human
intervention, express their viewpoint, or contest the decision?",
        "Is the continuous tracking of riders' data (like geolocation at 15-
second intervals) necessary and proportionate for the service, and is that data
protected and not retained longer than needed?"
      ],
      "expected_answers": [
        {
          "question": "Are riders provided with clear information about the
algorithmic systems that assign orders and evaluate performance, including the
main parameters and criteria used?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["LACK_TRANSPARENCY"],
          "gdpr_refs": ["13", "14", "5(1)(a)"],
          "rationale": [
            "The Garante explicitly found Foodinho had not adequately informed
riders about how the algorithms function [11]. That's a direct transparency
failure. If at audit time this hasn't been remedied, it's a clear violation.",
            "GDPR requires even employees be told about automated processing of
their data. Moreover, with decisions significantly affecting them, the
information should include logic per Art.13(2)(f). Initially, riders were in the
dark, which is non-compliance.",
            "Unless we see updated privacy notices or training materials given
to riders explaining the algorithm, we mark this as FAIL on transparency."
          ]
        },
        {
          "question": "Has the company implemented measures to ensure that data
feeding the algorithm (GPS data, delivery times, customer ratings, etc.) is
accurate and that any errors or biases (e.g. unfair negative ratings) do not
unduly affect riders' scores?",
```

```
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["INACCURATE_INPUT_DATA",
"ALGORITHM_BIAS"],
          "gdpr_refs": ["5(1)(d)", "5(1)(a)"],
          "rationale": [
            "One of Garante's orders was to check accuracy and relevance of all
data used by the algorithm, implying that previously this wasn't done. Riders
could be penalized by inaccurate or biased data (like GPS glitches or
discriminatory ratings).",
            "If the company hasn't introduced data cleansing, verification
steps, or bias corrections, it's still in violation of the data accuracy
principle and potentially fairness. For example, not filtering out obviously
false customer feedback or not accounting for technical issues would continue to
unfairly harm riders.",
            "We'd expect to see, post-investigation, processes like review of
outlier data, adjustment of ratings for context, etc. If those are absent, the
violation persists. Thus, likely FAIL at time of audit if no substantive
improvements were made."
          ]
        },
        {
          "question": "If the algorithm reduces a rider's job opportunities
(e.g. fewer orders or shifts) or deactivates them, is there a mechanism for the
rider to request human intervention, express their viewpoint, or contest the
decision?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["NO_HUMAN_REVIEW_PROCESS"],
          "gdpr_refs": ["22(3)"],
          "rationale": [
            "Garante found Foodinho had no procedure to enforce the right to
human intervention or contestation of automated decisions. That's a direct
breach of Article 22(3) for those decisions in scope.",

"If by now the company hasn't instituted an appeals process or a way for riders
to question the algorithm's decisions (like an email or support channel where a
human will actually review a complaint about the algorithmic outcome), it's non-
compliant.",
            "Given this was a core issue in the fine, absence of a remedy would
be a serious ongoing violation. We mark FAIL if no such mechanism exists or if
it's nominal (e.g., riders can complain but it goes nowhere)."
          ]
        },
        {
          "question": "Is the continuous tracking of riders' data (like
geolocation at 15-second intervals) necessary and proportionate for the service,
and is that data protected and not retained longer than needed?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["EXCESSIVE_TRACKING",
```

```
"UNDEFINED_RETENTION"],
          "gdpr_refs": ["5(1)(c)", "5(1)(e)", "32"],
          "rationale": [
            "The DPA highlighted very granular GPS tracking (every 15 seconds). This may be more than necessary for performance monitoring. We need to assess if the company adjusted this practice.",
            "If continuous tracking is still happening, we ask: is it truly needed? Possibly for route optimization, but maybe not at that frequency. Also, how long do they keep this location log? If indefinitely, that’s a retention violation.",
            "We flag NEEDS_REVIEW: if an audit finds they now delete location data after a short time or reduce frequency when idle, etc., it might be okay. If nothing changed, it’s excessive. We’d likely recommend they justify the necessity or dial it back, aligning with data minimization."
          ]
        }
      ],
      "ambiguity_notes": "This case intertwined labor rights and GDPR. The Garante applied GDPR principles but also Italian labor laws that require transparency of automated systems to workers. One ambiguity is the extent of 'meaningful information' about algorithms employees should get – the DPA clearly expects quite some detail (beyond generic statements). Additionally, balancing efficiency vs. privacy in tracking: companies argue frequent GPS pings are needed for service quality; regulators ask for justification. The precise threshold of 'necessary' tracking isn’t defined. Post-case, Glovo likely had to involve their DPO and perhaps worker reps in an ongoing algorithm audit, which is a new governance demand not explicitly spelled out in GDPR but derived from its accountability and fairness principles."
    },
    {
      "id": "gs_012",
      "title": "Italian Garante – Deliveroo Italy Algorithmic Management Fine",
      "authority": "Garante (Italian Data Protection Authority)",
      "jurisdiction": "Italy",
      "date": "22 July 2021",
      "source_url": "https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675422",
      "excerpt": "Deliveroo Italy was fined €2.5 million for GDPR violations in its algorithmic management of riders. The DPA found Deliveroo collected a disproportionate amount of data and was not sufficiently transparent about the algorithms used to manage its riders (both for assigning orders and for booking work shifts) [86]. The company also had to implement measures to periodically verify the correctness and accuracy of its algorithmic results, and to ensure compliance with transparency requirements.",
      "ai_relevance_tags": ["automated_decision", "employment", "transparency", "accuracy", "data_minimization"],
      "facts_summary": [
        "Deliveroo Italy’s platform used algorithms to allocate orders and
```

```
schedule riders, similar to Foodinho/Glovo. The Garante’s investigation in 2021 mirrored issues found with Foodinho.",

"**Excessive data collection:** Deliveroo gathered very detailed data on ~8,000 riders (likely constant geolocation, extensive performance metrics) – deemed disproportionate [86]. Much of this data was not strictly necessary for delivering pizza!",
        "**Lack of transparency:** Riders were not clearly informed about how these algorithms operated and impacted their work. The privacy information provided was inconsistent and insufficient.",
        "**Accuracy and fairness:** The DPA noted that Deliveroo needed to verify and ensure the algorithm’s outputs were correct and fair, similar to Foodinho’s mandate. Penalties or priority scores had to be based on accurate data.",

"Deliveroo was ordered to *improve transparency* (update privacy notices and rider communications to explain algorithm criteria) and to *audit its algorithms regularly* for accuracy and bias. They also had to **reduce data collection** to only what's necessary and delete irrelevant data.",
        "This case reinforced that gig economy algorithms fall under GDPR and national labor frameworks, requiring human-centric adjustments. Deliveroo reportedly complied by adjusting its data practices and providing more info to riders (and eliminating an unlawful “ranking” system that penalized low acceptance rates)."
      ],
      "questions": [

"Does the company limit the personal data collected on riders to what is necessary for operating the delivery service, or is it collecting excessive data (continuous tracking, exhaustive performance logs beyond necessity)?",
        "Has the company updated its privacy notices and internal policies to clearly explain to riders how the dispatch and scheduling algorithms work (at least the main factors and logic) and on what data these decisions rely?",
        "Are there processes in place to regularly evaluate and correct the algorithm’s decisions (ensuring they are based on accurate data and not producing unjustified penalties or exclusions)?"
      ],
      "expected_answers": [
        {
          "question": "Does the company limit the personal data collected on riders to what is necessary for operating the delivery service, or is it collecting excessive data (continuous tracking, exhaustive performance logs beyond necessity)?",
          "expected_verdict": "FAIL",
          "expected_violation_signals": ["EXCESSIVE_DATA_COLLECTION"],
          "gdpr_refs": ["5(1)(c)"],
          "rationale": [
            "The DPA found Deliveroo’s data collection disproportionate [86]. If
```

```
at audit we still see 24/7 tracking or very granular metrics not needed for pay or safety, that’s a data minimization breach.",
            "Necessary data might include when an order was delivered or maybe GPS during an active delivery. Anything beyond (like tracking even when not working, or storing super-detailed logs indefinitely) is excessive.",
            "Unless Deliveroo significantly dialed back data collection after 2021, we’d mark FAIL. This was a major point in the fine, so continued over-collection would indicate non-compliance."
          ]
        },
        {
          "question": "Has the company updated its privacy notices and internal policies to clearly explain to riders how the dispatch and scheduling algorithms work (at least the main factors and logic) and on what data these decisions rely?",
          "expected_verdict": "PASS",
          "expected_violation_signals": [],
          "gdpr_refs": ["13", "14"],
          "rationale": [

"Post-investigation, Deliveroo presumably had to rewrite its privacy disclosure. If we see a rider-facing notice saying: “Order assignment considers your location, delivery history, acceptance rate, etc.”, that’s compliance with transparency.",
            "The DPA specifically required transparency improvements. If Deliveroo implemented that (which is likely to avoid further fines), then we can mark this aspect as PASS – no continuing violation signal.",
            "We’d verify actual documents or rider feedback, but given the order, we expect they now meet the baseline of informing riders about algorithm criteria. Thus, no transparency signal if that’s in place."
          ]
        },
        {
          "question": "Are there processes in place to regularly evaluate and correct the algorithm’s decisions (ensuring they are based on accurate data and not producing unjustified penalties or exclusions)?",
          "expected_verdict": "NEEDS_REVIEW",
          "expected_violation_signals": ["LACK_OF_ALGO_AUDIT"],
          "gdpr_refs": ["5(1)(a)", "5(1)(d)"],
          "rationale": [
            "The Garante wanted Deliveroo to implement periodic checks on algorithm outputs. This implies ongoing algorithm auditing for accuracy/fairness.",

"We need to review if Deliveroo set up, say, a team or a process for this. It’s not a one-time fix; it’s continuous monitoring (maybe with DPO oversight). If no such governance exists, issues could persist unseen.",
            "We mark NEEDS_REVIEW. We’d expect to see some evidence: e.g.,
```

```
internal audit reports, adjustments made after finding a bias. If nothing, then that’s a concern (violation of accountability and potentially fairness). If they do have it, then good. So it requires examination."
          ]
        }
      ],
      "ambiguity_notes": "Like the Foodinho case, this mixes GDPR with new labour protections (Italy had just passed a law on transparency in algorithms for gig workers). The exact level of detail required in explanations is evolving – companies fear giving away algorithm IP, but regulators demand enough info for workers to understand how to improve their standing. Also, measuring 'accuracy' of an algorithm in workforce context is tricky – it involves fairness judgments. The DPA essentially asked for algorithmic audits, which is a newer concept in GDPR enforcement. Ensuring ongoing compliance is ambiguous: how frequently must they audit? Must results be shared? These are open questions that likely will be refined over time."
    }
  ],
  "signal_taxonomy": [
    {
      "signal": "NO_LAWFUL_BASIS",
      "definition": "Processing personal data without any valid legal basis under GDPR Article 6 (e.g., no consent, contract, legitimate interest, etc.), rendering the processing unlawful."
    },
    {
      "signal": "SPECIAL_DATA_NO_CONDITION",
      "definition": "Processing special category data (sensitive data as per Article 9) without meeting one of the conditions in Article 9(2) (e.g., no explicit consent for sensitive data)."
    },
    {
      "signal": "INVALID_CONSENT",
      "definition": "Relying on consent that is not GDPR-compliant (not freely given, specific, informed, and unambiguous). Also covers cases where consent should have been obtained but was not."
    },
    {
      "signal": "LACK_TRANSPARENCY",
      "definition": "Failing to provide clear and sufficient information to individuals about the processing (violating Articles 12–14). The data subject is effectively kept in the dark about significant processing aspects."
    },
    {
      "signal": "NO_ART14_NOTICE",
      "definition": "When personal data is obtained indirectly (not from the individual) and the controller does not provide the Article 14 notice in the required time frame and manner, without a valid exemption."
```

```
    },
    {
      "signal": "PURPOSE_CREEP",
      "definition": "Using personal data for new purposes that are incompatible with the original purpose for which data was collected, without obtaining new consent or meeting an Art.6(4) exemption."
    },
    {
      "signal": "EXCESSIVE_DATA_COLLECTION",
      "definition": "Collecting personal data beyond what is necessary for the specified purpose, breaching data minimization (Art.5(1)(c)). This includes overly granular or continuous data collection that is not justified."
    },
    {
      "signal": "UNLIMITED_RETENTION",
      "definition": "Retaining personal data for an indefinite or unjustifiably long period, contrary to the storage limitation principle (Art.5(1)(e)). No clear deletion schedule or retention policy exists."
    },
    {
      "signal": "INACCURATE_INPUT_DATA",
      "definition": "Using or generating personal data that is factually incorrect, outdated, or of poor quality, in violation of the accuracy principle (Art.5(1)(d)). Includes failing to correct known data errors."
    },
    {
      "signal": "DATA_ACCURACY_ISSUES",
      "definition": "A broader flag for any issues related to accuracy – either of input data or output (decisions/recommendations about individuals that may be based on incorrect data or yield incorrect info about them)."
    },
    {
      "signal": "BIAS_RISK",
      "definition": "Evidence that the AI system's outcomes may be biased or discriminatory against certain groups or individuals, compromising the fairness aspect of processing (Art.5(1)(a))."
    },
    {
      "signal": "SOLELY_AUTOMATED_DECISION",
      "definition": "Identification of a decision-making process that is fully automated with no meaningful human involvement, which has significant effects on individuals, potentially violating Article 22(1) if no exception/safeguards."
    },
    {
      "signal": "NO_HUMAN_INTERVENTION",
      "definition": "No mechanism for human review in an automated decision process where one is warranted (Art.22(3)). Data subjects cannot have a human override or assessment of an algorithmic decision that affects them."
```

```
    },
    {
      "signal": "DSR_NOT_HONORED",
      "definition": "Data subject rights were not respected – e.g., access,
erasure, rectification requests were ignored or denied unlawfully. Also covers
failing to facilitate rights (Art.12(2))."
    },
    {
      "signal": "DSR_OBSTRUCTION",
      "definition": "Any practice that impedes data subjects from exercising
their GDPR rights. For instance, not providing a channel to submit requests,
excessive delays, or blanket refusals without valid basis."
    },
    {
      "signal": "NO_EU_REPRESENTATIVE",
      "definition": "For a controller not established in the EU but subject to
GDPR (offering goods/services or monitoring in EU), failing to designate an EU
representative (Art.27)."
    },
    {
      "signal": "NON_COOPERATION",
      "definition": "Lack of cooperation with supervisory authorities (e.g.,
ignoring formal notices, refusing to answer inquiries), violating Article 31.
This often aggravates enforcement."
    },
    {
      "signal": "MISCLASSIFIED_SENSITIVE_DATA",
      "definition": "Controller did not recognize that data it is processing/
inferencing falls under special categories and thus failed to apply the required
stricter safeguards (treating sensitive inferences as regular data)."
    },
    {
      "signal": "POTENTIAL_COMPENSATION_RISK",
      "definition": "Indicates that a GDPR infringement could lead to damage
claims by individuals (Article 82). Not a direct violation itself, but flags
legal risk – e.g., profiling that causes distress might open the door to
compensation."
    },
    {
      "signal": "UNVERIFIED_14-5b_EXEMPTION",
      "definition": "The controller invoked the 'disproportionate effort'
exemption under Article 14(5)(b) to not inform data subjects, but it’s
questionable whether all conditions for that exemption are truly met."
    },
    {
      "signal": "NO_EXPLANATION_PROVIDED",
      "definition": "Data subjects impacted by an automated decision were not
given an explanation or the logic of the decision, despite requesting it or
```

```
expecting it under transparency/Art.15/22 rights (not fulfilling the 'meaningful information about logic' requirement)."
    },
    {
      "signal": "DSR_ACCESS_DENIED",
      "definition": "Failure to properly respond to an access request – either by outright denying access to personal data or algorithmic information that should be provided, or by providing an incomplete response without valid justification."
    },
    {
      "signal": "MISSING_CONSENT_SECONDARY_USE",
      "definition": "The controller is using personal data for a secondary purpose that is not strictly necessary for the service (often marketing or improvement) without obtaining consent when consent would be required (under GDPR or ePrivacy)."
    },
    {
      "signal": "BIOMETRIC_NO_CONSENT",
      "definition": "Biometric data (e.g., voice/facial recognition for identification) is processed without explicit consent or a lawful Art.9(2) exception. Essentially a special-case of SPECIAL_DATA_NO_CONDITION for biometric contexts."
    },
    {
      "signal": "PROFILING_NO_CONSENT",
      "definition": "Profiling (especially for marketing or ads) is conducted without an appropriate lawful basis (often lacking consent where it’s required under GDPR or ePrivacy, such as profiling via cookies or tracking)."
    },
    {
      "signal": "EXCESSIVE_TRACKING",
      "definition":
"Monitoring individuals (employees or users) in a continuous or overly intrusive manner that is not justified. E.g., very high-frequency location tracking or audio recording that overshoots necessity."
    },
    {
      "signal": "UNDEFINED_RETENTION",
      "definition":
"The controller has not defined a clear retention period for personal data, implying data might be kept indefinitely. A policy gap that likely leads to storage limitation breaches."
    },
    {
      "signal": "NO_HUMAN_REVIEW_PROCESS",
      "definition": "No established process for human intervention in automated decisions. Even if theoretically offered, in practice data subjects have no
```

```
clear way or procedural guarantee to have a human review an algorithmic
decision."
    },
    {
      "signal": "LACK_OF_ALGO_AUDIT",
      "definition":
"The organization lacks a procedure to audit and monitor its AI/algorithm
performance for errors, bias, or compliance over time. Essentially, no one is
periodically checking if the algorithm's outcomes remain lawful and accurate."
    }
  ]
}
```


---

1 2 3 4 5 6 Article 29 Working Party Guidelines on Automated Decision-Making and Profiling - Bird & Bird
https://www.twobirds.com/en/insights/2017/global/article-29-working-party-guidelines-on-automated-decision-making-and-profiling

7 Dutch government fraud scandal leads to record-breaking GDPR fine
https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/04/dutch-government-fraud-scandal-leads-to-record-breaking-gdpr-fin.html

8 9 60 63 72 How do we ensure lawfulness in AI? | ICO
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/

10 ICO takes enforcement action against HMRC in respect of biometric data - Birketts
https://www.birketts.co.uk/legal-update/ico-takes-enforcement-action-against-hmrc-in-respect-of-biometric-data/

11 RIDERS: ITALIAN SA SAYS NO TO ALGORITHMS CAUSING DISCRIMINATION A platform in the Glovo group fined EUR 2.6 million | European Data Protection Board
https://www.edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en

12 13 14 15 16 17 18 19 20 21 22 23 25 edpb.europa.eu
https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

24 30 31 AI: the Italian Supervisory Authority fines company behind chatbot "Replika" | European Data Protection Board
https://www.edpb.europa.eu/news/national-news/2025/ai-italian-supervisory-authority-fines-company-behind-chatbot-replika_en

26 Italian Garante bans Chat GPT from processing personal data of ...
https://www.dataprotectionreport.com/2023/04/italian-garante-bans-chat-gpt-from-processing-personal-data-of-italian-data-subjects/

27 Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di...
https://gpdp.it/garante/doc.jsp?ID=9870847

28 Press room - Garante privacy en
https://www.garanteprivacy.it/web/garante-privacy-en/press-room

29 [PDF] ChatGPT From a Data Protection Perspective
https://bsulawreview.org/wp-content/uploads/2024/04/10BSULawRev1.1.pdf

32 Italy's data watchdog fines AI company Replika's developer $5.6 ...
https://www.reuters.com/sustainability/boards-policy-regulation/italys-data-watchdog-fines-ai-company-replikas-developer-56-million-2025-05-19/

33 34 35 36 The French SA fines Clearview AI EUR 20 million | European Data Protection Board
https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

37 38 39 40 41 42 43 44 45 46 47 Facial recognition: Italian SA fines Clearview AI EUR 20 million | European Data Protection Board
https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

48 49 50 51 52 54 55 56 58 AI system development: CNIL’s recommendations to comply with the GDPR | CNIL
https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr

53 CNIL Clarifies GDPR Basis for AI Training – But It's Just ... - Skadden
https://www.skadden.com/insights/publications/2025/06/cnil-clarifies-gdpr-basis-for-ai-training

57 82 83 84 edpb.europa.eu
https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf

59 65 67 68 70 85 About this guidance | ICO
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/about-this-guidance/

61 62 64 66 69 71 How do we ensure transparency in AI? | ICO
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-transparency-in-ai/

73 74 75 76 77 78 79 EU Law Analysis: The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making
http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html

80 81 Groundbreaking Decision in Europe: CJEU Denies a Minimum Threshold for Raising Non-Monetary GDPR Damage Claims
https://www.orrick.com/en/Insights/2023/05/CJEU-Denies-a-Minimum-Threshold-for-Raising-Non-Monetary-GDPR-Damage-Claims

86 Italian data protection supervisory authority fines two food delivery companies for non-compliant algorithmic processing
https://www.aoshearman.com/en/insights/ao-shearman-on-data/italian-data-protection-authority-fines-2-food-delivery-companies-non-compliant-processing