

Country visit on 3 March 2025 – follow up information

JUSTICE SYSTEM

8. *As regards the examination of constitutionality of certain aspects of the administrative procedural code linked to legal aid in administrative cases (para §8a Verwaltungsgerichtsverfahrenssetz, see decision E 119/2023 of 12 December 2023 of the Constitutional Court), would you be able to update us on the state of play of these proceedings?*

Reference is made to the following decision of the Austrian Constitutional Court: VfGH 3.10.2024, [G 3504/2023](#).

9. *As regards the resources for the judiciary, would you have any estimation when a budget for 2025 can be expected? Following up to what was provided in your written input, could you elaborate on the progress made in filling existing vacancies, including at the Federal Finance Court? [figures can be provided in writing]*

Ministry of Justice

No concrete timetable for the budget negotiations has yet been announced. However, it is expected that the budget will be approved before the summer.

Because of various measures taken to attract and recruit staff and to strengthen the long-term loyalty of employees to the justice system, it has been possible to significantly increase the proportion of posts actually filled and maintain it at a very high level despite a significant increase in the number of available posts (257 posts in the last two years). As of 1 January 2025, the status of posts filled in courts and public prosecutors' offices is as follows¹:

	Posts filled in %
Judges	99,24 %
Public Prosecutors	98,38 %
Court Staff	99,75 %

Federal Finance Court

Judges:

As of 31.12.2024/01.01.2025, out of a total of 224 judges' posts (excluding president and vice-president), 183 were filled and 41 posts were vacant.

Development from 31.12.2023 to 31.12.2024:

Departures: 13 judges

Additions: 16 judges

Outlook for 2025: 14 judges are expected to retire in 2025. In 2024, there was a call for additional 13 posts for judges; on 03.02.2025, those 13 judges have taken up their duties. In addition, on 03.02.2025, another call for applications for 18 judges' posts was launched (planned appointment: December 2025).

¹ Including the Supreme Court and the General Procurator's Office, excluding the Federal Administrative Court.

Staff:

As of 31.12.2024/1.1.2025: 61 out of a total of 76 positions were filled; employees within the meaning of the question include five legal assistants.

Development from 31.12.2023 to 31.12.2024:

Departures: 4 employees

Additions: 13 employees (5x subject matter experts [Fachexperten], 5x legal assistants [juristische Mitarbeiter:innen], 1x policy officer [Fachreferent:innen], 2x assistants); these figures do not include assignments during the year and do not include legal and administrative interns nor maternity leave representation.

Outlook for 2025: There are no expected retirements. The process of filling further vacancies for administrative staff (as recommended by the Austrian Court of Audit on its report "BUND 2021/1") is ongoing.

10. Could you further elaborate on the state of play of implementation of the Justice 3.0 project, in particular what still remains outstanding in terms of courts/prosecution offices where the digital proceedings still need to be rolled-out? [figures can be provided in writing]

The strategic initiative „Justice 3.0“ manifests itself in introduction of digital proceedings throughout the judiciary. To further detail and update the already provided information on the state of play of implementation of the Justice 3.0 project a review of 2024 and an outlook to 2025 will be given.

Numerous important milestones were reached in 2024 and the Justice 3.0 rollout continued successfully:

- Completion of the rollout in appeal proceedings (civil) at the Higher Regional Courts
- Completion of the rollout in appeal proceedings (criminal) at the Regional Courts
- Completion of the rollout in conditional release proceedings
- Completion of the rollout in judicial administration proceedings
- Completion of the rollout of the payment order procedure
- Completion of piloting and start of the rollout in enforcement proceedings
- Start of piloting insolvency proceedings
- Start of piloting custody proceedings

In addition, more than 3 million proceedings are already digitally handled in the Justice 3.0 systems in January 2025. These include more than 50 million documents with a total of 200 million pages and already enable more than 100,000 electronic file inspections per month by parties, party representatives, experts and many more.

The digital justice workplace is available at a total of 160 offices, which means that 75% of the monthly nationwide new cases in the justice system are already managed digitally. The rollout of Justice 3.0 will continue in 2025, and the following milestones are targeted:

- Completion of the rollout in appeal proceedings (criminal) at the Higher Regional Courts
- Completion of the rollout in enforcement proceedings
- Completion of piloting and rollout in custody proceedings
- Completion of piloting and rollout in insolvency proceedings
- Piloting and rollout in inheritance proceedings
- Completion of the analyses of digital file management at the Supreme Court and Procurator General's Office

- Start of piloting digital file management at the Federal administrative court

By constantly working on Justice 3.0 more than 90% of new cases will be managed digitally by the end of 2025.

For the year 2026 the following rollout steps remain:

- Piloting and rollout at the Supreme Court, Procurator General's Office and Legal Protection Officer
- Completion of the rollout at the Federal administrative court
- Completion of the rollout of proceeding types with (very) low numbers of cases at the level of the Higher Regional Courts, e.g. cartel, disciplinary, patent and trademark cases
- Completion of the rollout of proceeding types with (very) low numbers of cases at the level of the regional courts and district courts, e.g. declarations of death, setting of deadlines

ANTI-CORRUPTION FRAMEWORK

5. *Following a ruling by the Austrian Constitutional Court in December 2023, the Austrian legislator regulated the seizure of digital data and data storage devices in an Act amending the Criminal Procedural Code in December 2024. Could you elaborate on the following:*

A) *Could you briefly summarise the main changes introduced by the new law and the reasoning behind the approach chosen, including the requirements to precisely define the categories of data to be seized? How do you view the implementation of these requirements in practice and their impact on the effectiveness of the investigations?*

Ministry of Justice

The new legal provisions on the seizure and analysis of digital data are based on the requirements set by the Court of Justice of the European Union (CJEU) and the Austrian Constitutional Court (VfGH). Both courts have imposed strict safeguards to protect personal data, which have been reflected in the revised legislation. Compared to other EU Member States, Austria acted swiftly by introducing the requirement of judicial authorization for data seizures within just two months after the CJEU ruling. This rapid legislative response demonstrates Austria's commitment to aligning its legal framework with European fundamental rights standards and ensuring compliance with the court's decision without unnecessary delays. While many other jurisdictions have yet to adapt their national laws accordingly, Austria has already implemented a clear and structured process, ensuring that digital investigations are conducted under judicial oversight and in full respect of proportionality and data protection principles.

The CJEU ruling (C-548/21) stipulates that access to data stored on mobile phones must meet the following conditions:

1. The nature or categories of the relevant offences must be clearly defined.
2. The principle of proportionality must be observed.
3. Except in emergency cases, data access must be approved by a court or an independent authority in advance.

In addition, the Austrian Constitutional Court (VfGH) imposed even stricter requirements. It ruled that whenever a court authorizes the seizure and subsequent analysis of digital data, it must specify:

- The categories of data that may be analyzed,

- The specific contents of the data that may be examined,
- The time period, and
- The investigative purposes for which the data may be used.

The VfGH also stated that merely obtaining a court order at the beginning of the process is not sufficient; a general assessment of proportionality alone does not suffice. Instead, the judicial authorization must explicitly define the specific parameters of the data. To comply with these rulings, the new law strengthens judicial oversight and introduces clear procedural safeguards while maintaining flexibility for effective investigations. The key changes include:

1. The law does not set a fixed list of offences for which data can be seized. This allows law enforcement to act flexibly based on the specific needs of each case while ensuring proportionality through case-by-case judicial review.
2. Before data can be examined, the prosecution must specify the data categories, contents, and time period they wish to analyze. The court must review these details and assess whether the measure is necessary and proportionate. This ensures greater judicial control over data access.
3. Emergency cases ("Gefahr im Verzug"): If there is an urgent need (e.g., risk of evidence destruction or immediate danger), law enforcement may temporarily seize a device and even access data before obtaining judicial approval. However, this measure must be fully documented, reported to the prosecution, and subsequently reviewed by a court. If the court denies authorization, the data must be deleted.
4. Data retention and expanded access: While only approved data can be analyzed initially, the full dataset is securely stored until the end of the criminal proceedings. If new evidence emerges and additional access is needed, the prosecution can request further judicial authorization to examine other parts of the dataset.
Both the "danger in delay" rule and the possibility of subsequent access to the full dataset ensure the effectiveness of criminal investigations. The danger in delay rule allows law enforcement to act immediately in urgent cases, preventing the loss of crucial evidence while ensuring that judicial review follows without unnecessary delays.
At the same time, the option to reassess the dataset at a later stage enables investigators to react flexibly to new developments in the case. This prevents situations where relevant evidence remains inaccessible simply because it was not initially identified as essential. Together, these provisions strike a balance between protecting fundamental rights and ensuring that law enforcement can effectively investigate.
5. Stronger rights for suspects and victims: The new law allows suspects and victims to request specific search parameters and, in some cases, to inspect the analyzed dataset. This strengthens the principle of fair trial (equality of arms) and victim rights, ensuring that digital evidence is not used unfairly.

In practice, these changes create a more structured and transparent process. While prosecutors must justify their requests more precisely, judicial oversight ensures that digital evidence is obtained lawfully and remains verifiable. The new rules impose higher procedural standards to meet the requirements set by the VfGH and the CJEU. While this demands greater precision and thorough justification, it also enhances trust and legal certainty, ensuring that criminal investigations are both effective and constitutionally sound.

Federal Bureau of Anti-Corruption

The implementation of the requirements in practice has become somewhat more challenging in terms of organisation and personnel. However, the effectiveness of the investigations is hardly affected.

- C) *We understand that under the amendments to the Criminal Code the Legal Protection Officer has been given a specific role in cases of data belonging to persons subject to professional privilege (e.g. lawyers) – could you elaborate on the role of the Legal Protection Officer in criminal proceedings in general, including on this new role following from the recent amendments, and clarify whether there are any possibilities to review the decision of the Legal Protection Officer in such cases?*

The Legal Protection Commissioner (LPO) is given tasks in order to exercise the special legal protection afforded by the Code of Criminal Procedure. Therefore the LPO is independent in the exercise of his or her duties and not bound by any directives. He or she is sworn to confidentiality. In particular, the LPO is responsible for assessing and controlling directions, authorizations, approvals, and the carrying out of specific investigative measure (e.g. data matching).

The Constitutional Court has emphasized the necessity of independent oversight in criminal proceedings to ensure that the interests of effective law enforcement are balanced with the protection of personal privacy and confidentiality. It has underscored that the legislature must implement effective control mechanisms to guarantee that law enforcement authorities strictly comply with court authorizations and legal provisions during data evaluation. This oversight is designed to safeguard the rights of affected individuals in a proportionate manner, even when they are not present during the review of their data. As an additional safeguard, this independent control complements the roles of both the LPO and the Data Protection Authority (DSB), reinforcing fundamental rights throughout the investigative process.

With the recent amendments, the LPO is responsible for overseeing the entire process related to digital evidence, from the seizure of data to its technical processing and final evaluation. The LPO ensures compliance with court-imposed conditions and the proper deletion of data after criminal proceedings conclude. Despite this broader scope of responsibilities, the role of the LPO does not interfere with the supervisory authority of the Data Protection Authority, which continues to oversee the public prosecution. The Data Protection Authority remains an independent institution ensuring that investigative measures comply with data protection laws, while the LPO provides an additional layer of scrutiny within the investigative process.

Importantly, the LPO is empowered to file complaints against court-approved investigative measures and to object to their implementation. However, there is no separate review mechanism for decisions made by the LPO. Instead, the LPO functions as an additional control instrument, with the authority to escalate concerns through legal remedies before the courts if any irregularities are detected. This means that the LPO's decisions are not subject to an independent review process but rather serve as a mechanism to trigger judicial oversight when necessary.

In conclusion, the amendments have strengthened the role of the LPO as a critical independent oversight body in the handling of digital evidence. By closely monitoring investigative measures, particularly those affecting privileged individuals, the LPO plays a crucial role in ensuring that legal safeguards are upheld throughout the criminal investigation process.

Update regarding resources of the Federal Bureau of Anti-Corruption:

The resources at the Federal Bureau of Anti-Corruption (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung, BAK) have increased (partly due to additional tasks which BAK has taken over starting January 2024). As mentioned in the AT Input 2024, the budget resources of the BAK have increased since 2014 and the implementation of projects and activities has been consistently assured. The BAK's expenditure budget in 2024 amounted to EUR 13,738 Mio. Following the National Council elections on September 29, 2024, an automatic provisional budget has come into force at the beginning of 2025 and the previous year's budget is going to be continued. Detailed figures to the budget of the BAK will be provided as soon as they are known. On 1 December 2024, the staff of the BAK included 174

employees (December 2023: 161), thirteen of whom are on maternity leave or work in other organizational units outside the BAK.

CHECKS AND BALANCES

4. *Could you provide us with a brief overview of the role of the Legal Protection Officer in the Austrian legal system, including as regards the appointment and dismissal? In addition, could you explain if there is any possibility to review the LPO's decisions?*

Please refer to our input for the Rule of Law Report 2020 for an overview of the role of the Legal Protection Officer (cf. page 55 et seq. on "The Commissioners for Legal Protection"): [European Rule of Law Mechanism - Austrian Input](#). This general information is still valid today, with the following update: the term of the LPO at the Federal Ministry of the Interior was extended to ten years (previously five years) with no possibility for renewal (section 91a SPG as amended with effect from 1 December 2021). Regarding the LPO at the Federal Ministry of Justice, please be informed in more detail as follows:

The LPO together with the necessary number of deputies is appointed for a period of three years by the Federal Minister of Justice after soliciting a joint proposal by the President of the Constitutional Court, the Chairperson of the Ombudsman Board (*Volksanwaltschaft*) and the President of the Conference of the Austrian Bar Associations. Reappointments are permissible.

It is a requirement that the LPO and deputies hold special knowledge and skills in the area of fundamental rights and freedoms and have worked for at least five years in a position for which a completed law degree is a professional prerequisite and in which they gained experience in criminal law and criminal procedure. Active judges and public prosecutors, registered attorneys and other persons who are excluded from or may not be appointed to the role of juror or lay assessor, may not be appointed as LPO or deputy.

The appointment of the LPO or the deputies lapses with their resignation, death, term of appointment or with any incompatibility within the meaning of the above occurring after their appointment. (Sec. 47a para. 1 to 3 of the Code of Criminal Procedure [*StPO*], in the following "CCP")

The LPO is given tasks in order to exercise the special legal protection afforded by the Code of Criminal Procedure. The LPO is independent in the exercise of his or her duties and not bound by any directives. He or she is sworn to confidentiality.

In particular, the LPO is responsible for examining and monitoring the ordering, authorisation, approval and implementation of

1. undercover investigations,
2. the conclusion of a sham transaction, if this is to be ordered by the public prosecutor's office,
3. optical and acoustic surveillance of persons,
4. automated data synchronisation and
5. investigative measures in connection with the seizure of letters, information on message transmission data, localisation of technical equipment and monitoring of messages as well as optical and acoustic surveillance of persons who are authorised to refuse to testify (Sec. 147 para. 1 CCP).

In certain cases, such as when the termination of preliminary proceedings relating to certain offences takes place in proceedings in which there is a particular public interest due to the

significance of the offence or the person of the accused, or in which legal questions of fundamental importance have not yet been sufficiently clarified, the LPO is entitled to submit a motion for continuation of investigation proceedings (Sec. 194 para. 3, Sec. 195 para. 2a CCP, cf. also Sec. 209a para. 6 CCP).

At the instigation of the LPO, the Procurator-General's Office may lodge an appeal for nullity 'to safeguard the law' against the unlawful execution of a coercive measure by the criminal investigation authorities or the unlawful authorisation of a coercive measure and against a decision by the prosecution authority about the conclusion of investigation proceedings, so long as a person entitled to seek legal redress has not sought such legal redress or if a person entitled to seek legal redress cannot be identified (Sec. 23 para. 1a CCP).

In the context of the seizure of data the Constitutional Court has emphasized the necessity of independent oversight in criminal proceedings to ensure that the interests of effective law enforcement are balanced with the protection of personal privacy and confidentiality. It has underscored that the legislature must implement effective control mechanisms to guarantee that law enforcement authorities strictly comply with court authorisations and legal provisions during data evaluation. This oversight is designed to safeguard the rights of affected individuals in a proportionate manner, even when they are not present during the review of their data. As an additional safeguard, this independent control complements the roles of both the LPO and the Data Protection Authority (*DSB*), reinforcing fundamental rights throughout the investigative process.

With the recent amendments, the LPO is responsible for overseeing the entire process related to digital evidence, from the seizure of data to its technical processing and final evaluation. The Legal Protection Commissioner ensures compliance with court-imposed conditions and the proper deletion of data after criminal proceedings conclude. Despite this broader scope of responsibilities, the role of the LPO does not interfere with the supervisory authority of the Data Protection Authority, which continues to oversee the public prosecution. The Data Protection Authority remains an independent institution ensuring that investigative measures comply with data protection laws, while the LPO provides an additional layer of scrutiny within the investigative process (Sec. 115I CCP).

In certain constellations the prosecuting officer must seek the LPO for authorisation before ordering certain types of investigative measures (see Sec. 144 para. 3 CCP, Sec. 147 para. 2 CCP and Sec. 115I para. 1 CCP referring to Sec. 155 para. 1 subpara. 1 and Sec. 157 para. 1 subpara. 2 to 4 CCP). The CCP provides for special protection in certain areas, such as the protection of confidentiality of clergy and of professional confidentiality. Therefore persons working in the areas mentioned in Sec. 157 para. 1 subpara. 2 to 4 CCP have the right of refusal to answer questions (e.g. defence counsel and attorneys on matters that come to their knowledge in that capacity); furthermore and as a consequence of that, these rights may not be circumvented by other investigative measures (Sec. 115I para. 1 in conjunction with Sec. 144 para. 3 CCP). The prohibition on circumventing e.g. the attorney-client privilege does not apply if the person himself or herself is strongly suspected of having committed the offence. In such cases, the authorisation of the LPO is required for the ordering and execution of investigative measures with respect to access to digital information. In these - and only in these - cases, the authorisation of the LPO is a prerequisite for the investigative measure.

To summarise, the LPO has a crucial role to play in ensuring compliance with legal safeguards throughout the criminal investigation process.

However, there is no separate review mechanism for decisions made by the LPO. Instead, the LPO acts as an independent and autonomous additional control instrument, with the authority to escalate concerns through legal remedies before the courts if any irregularities are detected

(Sec. 147 para. 2 to 4 CCP, cf. also Sec. 115I CCP regarding seizure of digital information). This means that the LPO decisions are not subject to an independent review process but rather serve as a mechanism to trigger judicial oversight when necessary.

By 31 March of each year, the LPO has to present a report to the Federal Minister of Justice about the LPO's activities and perceptions within the exercise of the LPO's function in the previous calendar year (Sec. 47a para. 7 CCP).