CONSTITUTIONAL COURT
G 352/2021-46
14 December 2023

IN THE NAME OF THE REPUBLIC

The Austrian Constitutional Court, chaired by President
Christoph GRABENWARTER,

in the presence of Vice-President
Verena MADNER

and the members
Markus ACHATZ,
Sieglinde GAHLEITNER,
Andreas HAUER,
Christoph HERBST,
Michael HOLOUBEK,
Claudia KAHR,
Michael MAYRHOFER,
Michael RAMI and
Ingrid SIESS-SCHERZ

as voting members, in the presence of the recording clerk
Josef MÜLLNER

decided today – after a public oral hearing held on 22 June 2023, having heard the presentation by the judge rapporteur and the statements by the applicant's representatives Richard Soyer, lawyer, and Philip Marsch, lawyer, the representatives of the Federal Government Johanna Hayden, Christian Manquet, Daniel Buchberger and Florian Rudolf as well as the resource person René Mayrhofer – pursuant to Article 140 of the Constitution (*Bundes-Verfassungsgesetz, B-VG*) on the application filed by *****, represented by Richard Soyer, lawyer, Kärntner Ring 6, 1010 Vienna, to repeal as unconstitutional section 110 paragraph 1 subparagraph 1 and paragraph 4 as well as section 111 paragraph 2 of the Code of Criminal Procedure (*Strafprozessordnung, StPO*):

I. Section 110 paragraph 1 subparagraph 1 and paragraph 4 as well as section 111 paragraph 2 of the Code of Criminal Procedure, Federal Law Gazette (*Bundesgesetzblatt*, *BGBl*.) 631/1975 as amended by Federal Law Gazette I no. 19/2004 are repealed as unconstitutional.

II. The provisions will be repealed with effect after 31 December 2024.

III. Previous legal provisions shall not re-enter into force.

IV. The Federal Chancellor is obliged to publish these rulings without delay in Federal Law Gazette I.

Reasoning

I. The Application

Based on Article 140 paragraph 1 subparagraph 1 point d of the Constitution (*B-VG*), the applicant requests that the Constitutional Court repeal as unconstitutional section 110 paragraph 1 subparagraph 1, section 110 paragraph 4 and section 111 paragraph 2 of the Code of Criminal Procedure 1975 (*Strafprozeßordnung 1975, StPO*), Federal Law Gazette 631/1975, as amended by Federal Law Gazette I 19/2004. In two alternative claims, the applicant requests the repeal of sections 110 to 114 Code of Criminal Procedure in various versions. 1

II. The Law

The relevant provisions of the Code of Criminal Procedure (*StPO*), Federal Law Gazette 631/1975 (re-publication), as amended by Federal Law Gazette I 243/2021, read as follows (the provisions as amended by Federal Law Gazette I 19/2004 challenged in the main claim are highlighted): 2

"Part 1
General provisions and principles of criminal proceedings

Chapter 1
General principles of criminal proceedings

Criminal proceedings

Section 1 (1) The Code of Criminal Procedure defines the proceedings for the investigation of criminal offences, for the prosecution of suspects and for related decisions. For the purposes of this Code, a criminal offence is any conduct punishable by judicial sanctions under laws at federal or *Länder* level.

(2) Criminal proceedings commence when criminal investigation or prosecution authorities begin to investigate a reasonable suspicion (*Anfangsverdacht*, paragraph 3) in accordance with the provisions of Part 2 of this Code; the proceedings shall be conducted as investigation proceedings against unknown perpetrators or against the suspect as long as a person is not specifically suspected by reason of certain facts of having committed an offence (section 48 paragraph 1 subparagraph 2); from that time onwards, the process shall be conducted as investigation proceedings against that person as the accused. Criminal proceedings end by discontinuation or withdrawal of the prosecution by the prosecution authority or by court decision.

(3) A reasonable suspicion exists if, on the basis of specific indications, there is reason to believe that a criminal offence has been committed.

[…]

Legality and proportionality

Section 5 (1) In exercising their powers and in taking evidence, criminal investigation authorities, prosecution authorities and the courts may only interfere with the rights of persons to the extent expressly provided for by law and as necessary to fulfil their duties. Any infringement of legally protected interests thus caused must be reasonably proportionate to the gravity of the criminal offence, the degree of suspicion and the outcome sought.

(2) Where multiple effective investigative and coercive measures are available, criminal investigation authorities, prosecution authorities and the courts shall choose the measure that least adversely affects the rights of the persons concerned. At any stage during the proceedings, powers assigned by law shall be exercised in a manner that avoids unnecessary attention, that respects the dignity of the persons concerned and safeguards their rights and interests requiring protection.

[…]

Chapter 5
Common provisions

Subchapter 1
Use of information technology

Processing of personal data

Section 74 (1) The criminal investigation authorities, the prosecution authorities and the courts may process relevant personal data in the course of their duties. Unless special provisions concerning the processing of personal data exist, the provisions of the Data Protection Act (*Datenschutzgesetz* [*DSG*], Federal Law Gazette 165/1999) apply.

(2) When processing personal data, the criminal investigation authorities, the prosecution authorities and the courts shall give due consideration to the principle of legality and proportionality (section 5). In any event, they shall safeguard the data subjects' secrecy interests that require protection and prioritize the confidential use of personal data. When processing special categories of personal data (section 39 Data Protection Act) and personal data relevant for criminal justice purposes, they shall take all reasonable steps to safeguard the secrecy interests of data subjects.

Rectification, erasure and blocking of personal data

Section 75 (1) Personal data that is inaccurate or incomplete or that was obtained in contravention of the provisions of this Code shall, *ex officio* or at the request of the data subject, be immediately rectified, completed or erased. The authorities and courts shall be notified of the rectification or erasure of any personal data previously transmitted to them (section 76 paragraph 4). The federal, *Land* and municipal authorities as well as public bodies and institutions established under public law from whom the data to be rectified originates shall also be notified of such rectification.

[…]

PART 2
Investigation proceedings

Chapter 6
General provisions

Subchapter 1
Purpose of investigation proceedings

Purpose of investigation proceedings

Section 91 (1) Investigation proceedings serve to investigate the facts of the case and the suspicion that a crime has been committed to the extent that the prosecution authority can decide whether to indict, withdraw the prosecution or discontinue the proceedings and, in the event of an indictment, to enable the trial (*Hauptverhandlung*) to be conducted expeditiously.

(2) Investigations involve any activities by the criminal investigation authority, the prosecution authority or the court intended to obtain, secure, evaluate or process information that serves to investigate the facts of a suspected criminal offence. Investigations shall be conducted in the form provided for by this Code either as inquiries or as evidence-taking. The mere use of publicly accessible sources of information or of sources of information internal to the authorities and the gathering of information to ascertain whether a reasonable suspicion (section 1 paragraph 3) exists, are not investigations within that meaning.

[…]

Chapter 7
Duties and powers of the criminal investigation authority, prosecution authority and of the court

[…]

Subchapter 4
The court’s role in investigation proceedings

[…]

Objection on grounds of violation of a right

Section 106 (1) Any person claiming to have their individual rights violated in investigation proceedings by the prosecution authority may bring an objection (*Einspruch*) before the court if
1. the exercise of a right under this Code has been refused or

2. an investigative or coercive measure has been ordered or executed in violation of provisions of this Code.
In the event of the death of the person entitled to bring the objection, this right passes to the relatives mentioned in section 65 subparagraph 1 point b. There is no violation of individual rights where the law does not establish a binding rule on the conduct of the prosecution authority or the criminal investigation authority and if this discretion was used within the spirit of the law.

(2) If a complaint (*Beschwerde*) is brought against the approval of an investigative measure, any objection brought against the ordering or execution of that measure must be combined with the complaint. In such a case, the court deciding on the complaint also decides on the objection.

(3) The person concerned shall lodge the objection with the prosecution authority within six weeks after becoming aware of the alleged violation of individual rights. The objection shall state the order or act concerned, the substance of the violation of rights and the remedy sought. If the objection concerns measures taken by the criminal investigation authority, the prosecution authority shall give the criminal investigation authority the opportunity to make a statement.

(4) The prosecution authority shall review whether the alleged violation of rights exists and, where the objection is justified, shall comply with the objection and notify the person who raised the objection of that assessment and in which way the objection was complied with and that the person nevertheless has the right to demand a decision by the court if the person claims that their objection was in fact not complied with.

(5) If the prosecution authority does not comply with the objection within four weeks or if the person who raised the objection demands a decision by the court, the prosecution authority shall refer the objection to the court without delay. The court shall serve statements by the prosecution authority and the criminal investigation authority on the person who raised the objection for comment within a period set by the court, not exceeding seven days.

[…]

Chapter 8
Investigative measures and taking of evidence

Subchapter 1
Securing or seizure of items, disclosure of information contained in the register of bank accounts and disclosure of information concerning bank accounts and banking transactions

Definitions

Section 109 For the purposes of this Code

1. ‘securing’ (*Sicherstellung*) of items means
a. establishment of temporary power of disposition over items and
b. a temporary prohibition on the surrender of items or other assets to third parties (third party prohibition, *Drittverbot*) and the temporary prohibition on the sale or pledging of such items or assets,
[…]

Securing

Section 110 (1) Items may be secured if it appears necessary
1. for evidentiary reasons,
2. to safeguard private law claims, or
3. to safeguard confiscation (*Konfiskation* – section 19a Criminal Code [*Strafgesetzbuch, StGB*]), forfeiture (*Verfall* – section 20 Criminal Code), extended forfeiture (section 20b Criminal Code), preventive confiscation by the court (*Einziehung* – section 26 Criminal Code) or any other property-law order provided by law.

(2) The prosecution authority makes the order to secure which is then executed by the criminal investigation authority.
[…]

(4) If and as soon as evidentiary requirements can be met through visual, audio or other recordings or by making copies of written records or electronically processed data and if it is not expected that the secured items themselves or the original versions of the secured information will be viewed during the trial, these items shall not be secured for evidentiary reasons (paragraph 1 subparagraph 1) and, if secured, shall in any case be released at the request of the person concerned.

Section 111 (1) Any person who has power of disposition over items or assets that are to be secured is obliged (section 93 paragraph 2) to surrender these at the request of the criminal investigation authority or enable them to be secured in another way. Where necessary, this obligation may be enforced by searching of persons or dwellings, applying by analogy sections 119 to 122.

(2) If information saved on data storage devices is to be secured, any person shall grant access to that information and, upon request, shall issue or produce an electronic data storage device in a commonly used file format. Furthermore, any person shall acquiesce to the making of backup copies of the information saved on the data storage device.
[…]

(4) In any case, confirmation that items or assets were secured shall be issued to or served on the person concerned immediately or within no more than 24 hours and the person shall be informed of the right to bring an objection (section 106) and to request a decision by the court to lift or continue the securing (section 115).

Where possible, victims shall be informed when items or assets are secured in order to safeguard enforcement of a decision on private law claims (section 110 paragraph 1 subparagraph 2).

Section 112 (1) If the person concerned by or present during the securing, even if that person is among those accused of the crime, objects to the securing of written records or data storage devices by invoking a legally recognized right to confidentiality that must not be circumvented by securing (otherwise the securing will be void), such records or devices shall be protected in an appropriate manner against unauthorized access and alteration and shall be deposited with the court. At the request of the person concerned, the records shall, however, be deposited with the prosecution authority where they shall be stored separately from the investigation file. In either case, neither the prosecution authority nor the criminal investigation authority shall access the records until a decision concerning access has been made pursuant to the following paragraphs.
[…]

(3) The person concerned may bring an objection against the order of the prosecution authority, in which case the records shall be presented to the court and the court shall decide whether and to what extent the records may be added to the file; paragraph 2 last sentence applies. Complaints against the court order have a suspensive effect.

Section 112a. (1) If an authority or public office concerned objects to the securing of written records or data storage devices on the grounds that
1. those records or devices contain information which, according to statutory provisions or under the Federal Security Code (*Geheimschutzordnung des Bundes, GehSO*) established pursuant to section 12 of the Federal Ministries Act (*Bundesministeriengesetz, BMG*) 1986, Federal Law Gazette 76/1986, constitutes classified intelligence information the secrecy of which overrides the interest in criminal prosecution in the individual case, or
2. those records or devices contain classified information transmitted by foreign security agencies or security organizations (section 2 paragraph 2 of the Police Cooperation Act [*Polizeikooperationsgesetz, PolKG*], Federal Law Gazette I 104/1997) which may be processed for purposes other than those for which it was transmitted only with the prior consent of those foreign security agencies or security organizations, the records or devices shall be protected in an appropriate manner against unauthorized access and alteration and shall be deposited with the court. Neither the prosecution authority nor the criminal investigation authority shall access the records or devices until a decision concerning access has been made pursuant to the following paragraphs.
[…]

(4) The authority or public office shall have the right to file a complaint against the court order; such complaint has a suspensive effect.

Section 113 (1) Securing ends

1. if it is lifted by the criminal investigation authority (paragraph 2),
2. if the prosecution authority orders that it be lifted (paragraph 3),
3. if the court orders seizure.

(2) The criminal investigation authority shall notify the prosecution authority of the securing of any items or assets without delay, at the most within 14 days (section 100 paragraph 2 subparagraph 2), unless the criminal investigation authority lifts a securing under section 110 paragraph 3 before such time because the requirements are not met or have ceased to apply. This notification may, however, be combined with the subsequent one if this does not infringe the material interests of the proceedings or of persons and if the secured item is of low value, is under nobody's power to dispose, or if possession of the item or asset is generally prohibited (section 445a paragraph 1). In cases under section 100 paragraph 3 subparagraph 4, the criminal investigation authority shall proceed pursuant to the provisions of sections 3, 4 and 6 of the Counterfeiting of Goods Act (*Produktpirateriegesetz, PPG)* 2004, Federal Law Gazette 56/2004.
[…]

(4) Secured items (section 109 subparagraph 1 point a) shall not be seized, not even on application, if the secured items fall within the meaning of section 110 paragraph 3 subparagraph 1 points a and d or subparagraph 2 or if the purpose for which the items were secured can be achieved through other measures by the authorities. In such cases the prosecution authority shall make the necessary disposition over the secured items and their continued storage and, where necessary, lift the securing of items.

Section 114 (1) The criminal investigation authority shall be responsible for storing secured items until it notifies the prosecution authority of the securing (section 113 paragraph 2) of items; thereafter, responsibility passes to the prosecution authority.

(2) If the grounds for continued storage of secured items cease to apply, the items shall immediately be returned to the person who had power of disposition over the items at the time they were secured, unless it is evident that this person is manifestly not authorized to have disposition. In this case, the items shall be transferred to the authorized person or, if no such person can be established or can only be established with disproportionate effort, the items may be deposited with the courts pursuant to section 1425 of the Civil Code (*Allgemeines bürgerliches Gesetzbuch, ABGB*). The persons concerned shall be notified accordingly.

Seizure

Section 115. (1) Seizure shall be permitted if it is expected that the secured items
1. will be needed as evidence in the further course of proceedings,
2. are the object of private law claims or

3. will serve to safeguard enforcement of a decision by the court concerning confiscation (section 19a Criminal Code), forfeiture (section 20 Criminal Code), extended forfeiture (section 20b Criminal Code), preventive confiscation (section 26 Criminal Code) or to safeguard any other property-law order provided by law, the enforcement of which would otherwise be jeopardized or significantly impeded.

(2) The court shall decide on seizure without delay upon application by the prosecution authority or by any person concerned by the securing.

(3) Section 110 paragraph 4 shall apply by analogy. Where relevant, the seizure shall be limited to the recordings and copies mentioned in section 110 paragraph 4.
[…]"

III. Initial Proceedings, Application and Preliminary Proceedings

1. The applicant is subject to criminal investigation proceedings (section 91 et seq. of the Code of Criminal Procedure) because of suspected dishonesty (*Untreue*, section 153 paragraph 1 and paragraph 3 first case Criminal Code). 3

2. On 21 July 2021, the Klagenfurt Prosecution Authority (*Staatsanwaltschaft Klagenfurt*) ordered the securing of the applicant's mobile phone and Outlook calendar. The applicant filed an objection on grounds of violation of a right (section 106 Code of Criminal Procedure) against this order alleging that the measure was disproportionate because a mobile phone provides unlimited access to a person's life circumstances and personal history, particularly as it can be used to access data stored in the cloud. 4

3. The Klagenfurt Regional Court (*Landesgericht Klagenfurt*) dismissed the objection on grounds of violation of a right in its decision of 4 November 2021. It argued that items may be secured only if this is deemed necessary and appropriate for the purpose to be achieved and that securing of such items must always be connected to a specific criminal matter. Securing of the mobile phone and Outlook calendar was necessary for evidentiary reasons, the Klagenfurt Regional Court found, and was also the least intrusive means available because the data concerning business meals and business trips stored in them served the investigation of a suspected criminal offence. 5

4. The applicant lodged a complaint against this decision with the Graz Higher Court of Appeal (*Oberlandesgericht Graz*) within the statutory time limit and brought the present application under Article 140 paragraph 1 subparagraph 1 point d of the Constitution. 6

4.1. The applicant argues that, in light of the wealth of data that a smartphone contains, deep insights into the life and private sphere of the person concerned is provided by the securing of a smartphone for evidentiary reasons. One look into the phone is enough to tell you all there is to know about the person. At the same time, all that is required for a mobile phone to be secured is an order by the prosecution authority in the course of criminal investigation proceedings, and in turn all that is required to initiate such proceedings is a reasonable suspicion (section 1 paragraph 3 Code of Criminal Procedure). All other investigative measures involving comparable interference are subject to more stringent substantive and formal requirements. This is the case, for example, with identity verification (*Identitätsfeststellung*) pursuant to section 118 Code of Criminal Procedure where certain facts must be present. Similar requirements apply for the disclosure of bank data (A*uskunft über Bankdaten*) under section 116 Code of Criminal Procedure, and in this case court approval is additionally required. Approval by the court is also required for searches of places and items (commonly referred to as *Hausdurchsuchung* - house searches, section 120 Code of Criminal Procedure) and molecular-genetic testing (*molekulargenetische Untersuchung*, section 124 Code of Criminal Procedure). Physical examinations (*körperliche Untersuchung*, section 123 Code of Criminal Procedure) may be carried out only if certain facts specified in the law are present, and additionally are subject to a stringent review of proportionality. Surveillance (*Observation)* and undercover investigations (*verdeckte Ermittlung;* section 130 et seq. Code of Criminal Procedure) are subject to stringent time limits. Section 134 et seq. Code of Criminal Procedure sets out detailed requirements for the seizure of letters (*Beschlagnahme von Briefen*), the disclosure of data concerning transmission of messages (*Auskunft über Daten einer Nachrichtenermittlung*) as well as the localizing of a technical device (*Lokalisierung einer technischen Einrichtung*) and the surveillance of messages (*Überwachung von Nachrichten*), with the approval of a judge being required in each case. In the case of undercover investigations and surveillance of encrypted communication (*Überwachung verschlüsselter Nachrichten*), section 147 Code of Criminal 7

Procedure provides for legal protection to be exercised by the Legal Protection Commissioner (*Rechtsschutzbeauftragter*).

4.2. By issuing a simple order to secure items, these detailed requirements may be circumvented, leaving a defendant without legal protection in the main proceedings (section 210 et seq. Code of Criminal Procedure) because such an order is not subject to any consequence of nullity. 8

4.3. As a result, the applicant argues, the securing of a mobile phone interferes disproportionately with rights under Article 8 of the European Convention on Human Rights (ECHR) and section 1 of the Data Protection Act (*Datenschutzgesetz, DSG*). This is the case, firstly, because the provisions of the law are not sufficiently specific, and secondly, because the securing of items – which permits unlimited interference with private life in terms of the time period and content concerned – can be ordered on minimal grounds, namely in the case of mere 'reasonable suspicion' and if the mobile phone is suitable for use as evidence in the proceedings. In this respect, the law also violates the principle of equal treatment (Article 2 of the Basic State Law [*Staatsgrundgesetz, StGG*] and Article 7 paragraph 1 of the Constitution [*B-VG*]) because the provisions of the Code of Criminal Procedure mentioned impose significant substantive and formal limitations on investigating authorities, which, however, do not apply when mobile phones are secured. 9

5. The Graz Higher Court of Appeal dismissed the complaint, which made reference to the application under Article 140 paragraph 1 subparagraph 1 point d of the Constitution that had been lodged simultaneously, by decision of 12 January 2022. 10

6. By letter of 27 January 2022, the Constitutional Court notified the Graz Higher Court of Appeal of the present application in accordance with section 62a paragraph 5 Constitutional Court Act (*Verfassungsgerichtshofgesetz, VfGG*). 11

7. The Procurator General's Office lodged a plea of nullity for the preservation of the law (*Nichtigkeitsbeschwerde zur Wahrung des Gesetzes*, section 23 Code of Criminal Procedure) against the decision of the Graz Higher Court of Appeal of 12 January 2022 with the Supreme Court of Justice (*Oberster Gerichtshof*), arguing that by reason of section 62a paragraph 6 Constitutional Court Act, the Graz 12

Higher Court of Appeal should not have given its decision before the decision of the Constitutional Court on the application pursuant to Article 140 paragraph 1 subparagraph 1 point d of the Constitution.

8. The Supreme Court of Justice (*Oberster Gerichtshof, OGH*) rejected the plea of nullity for the preservation of the law by judgment of 31 May 2022, *****, finding that the appellate court's obligation to stay proceedings pursuant to section 62a paragraph 6 Constitutional Court Act is triggered only by a notification of the Constitutional Court in accordance with section 62a paragraph 5 first sentence Constitutional Court Act and not by a mere reference made by the appellant. 13

9. The Federal Government submitted written observations contesting the admissibility of the application and denying the applicant's constitutional concerns. 14

9.1. It argued that the securing of a data storage device does not necessarily entail evaluation of the data because a separate order is required for that. In response to the applicant's argument regarding the supposedly unlimited nature of the interference, the Federal Government observes that the investigating authorities evaluate data for criminal prosecution purposes only and are not permitted to place on file information which is not relevant for criminal justice purposes (cf. section 74 paragraph 1 Code of Criminal Procedure; *OGH 13.10.2020*, 11 Os 56/20z). Data collected in violation of the provisions of the Code of Criminal Procedure 1975 must be erased *ex officio* or on application (section 75 paragraph 1 Code of Criminal Procedure). The items into which the data storage device is incorporated need not necessarily be secured, nor is it necessary to secure the data storage device on which the relevant data was originally saved; otherwise the obligation to permit investigating authorities access to saved data as provided for in section 111 paragraph 2 Code of Criminal Procedure would be devoid of purpose, especially when external storage is used (*OGH 11.9.2018, 14 Os 51/18h*). In addition, the law enforcement authorities are not permitted to use the secured device to access data stored remotely after the device has been secured. They must close all connections and put the phone into flight mode so that the only data secured is the data accessible at the time of securing the device (Zerbes, *Beweisquelle Handy. Ermittlungen zwischen Sicherstellung und Nachrichtenüberwachung, ÖJZ 2021*, 176 [180]). Furthermore, the European Court of Human Rights (ECtHR) has already previously found that prosecutors are permitted to view that 15

material when a large volume of data is seized (ECtHR, 4 June 2019, 39757/15, *Sigurður Einarsson v. Iceland*, paragraph 90).

9.2. In accordance with section 1 paragraph 3 Code of Criminal Procedure, a reasonable suspicion, meaning specific indications giving reason to believe that a criminal offence has been committed, is required for an item to be secured. The "certain facts" cited by the applicant and mentioned in other provisions refer to precisely this reasonable suspicion, as the example of identity verification pursuant to section 118 Code of Criminal Procedure shows. In addition, grounds for ordering the securing of items must be specified: It must be shown which items are to be secured and how those items are relevant. Moreover, the principle of proportionality pursuant to section 5 paragraphs 1 and 2 Code of Criminal Procedure, with due regard for provisions relating to fundamental rights, especially Article 8 ECHR and section 1 Data Protection Act, must be observed when securing items (*OGH 28.7.2020, 11 Os 51/20i; 13.10.2020, 11 Os 56/20z*), in contravention of which the person concerned can resort to the remedy of objection to enforce these rights. 16

9.3. Furthermore, securing is a temporary measure only. Approval by a judge is only required for the subsequent seizure of the items concerned, and the person concerned can request a decision by the court to lift or continue the securing under section 115 Code of Criminal Procedure. 17

9.4. The surveillance measures under section 130 et seq. Code of Criminal Procedure referred to in the application differ fundamentally from the securing of a data storage device. Surveillance measures are usually carried out covertly, and surveillance of a person's activities without their knowledge is typically done over a certain period of time, while in the case of securing of items only a momentary snapshot is made. Surveillance can only be carried out in real time and requires the involvement of a third party, i.e. the communication service provider. Once the data is within the sphere of a certain user, that data is at the user's disposal, and the data is subject to securing. This means that the level of protection applicable in such a case differs from that connected to the confidence in the integrity of the means of communication (which is protected by the secrecy of telecommunications), and the law differs accordingly. Moreover, the European Court of Human Rights found that subsequent judicial review offered sufficient protection even in 18

the case of (secret) surveillance measures (ECtHR, 2 September 2010, 35623/05, *Uzun v. Germany*, paragraphs 71 to 74; 12 January 2016, 37138/14, *Szabó and Vissy v. Hungary,* paragraph 77).

9.5. As regards the applicant's additional claim that, in view of the diversity of data concerned, provisions specifically addressing the securing of smartphones are required, the applicant is asking the legislator to draw a distinction according to the potential evidentiary value of a secured item – which is impossible in practice because this would mean that the result of an investigation must be anticipated. Although a smartphone of course contains a wealth of accumulated information, it would be possible to acquire this information by securing other items, perhaps several of them (notebooks, diaries, etc.). Consequently, it would appear unjustified to make the securing of a mobile phone subject to more stringent requirements than the securing of other personal belongings. 19

10. The Constitutional Court held a public oral hearing on 22 June 2023, during which technical, practical and legal issues connected with the provisions challenged were discussed with the parties. 20

IV. Considerations

1. **As to the admissibility** 21

1.1. In accordance with Article 140 paragraph 1 subparagraph 1 point d of the Constitution (*B-VG*), the Constitutional Court decides on the unconstitutionality of laws on application by a person being a party to a case that has been decided by an ordinary court at first instance who alleges infringement of their rights because of the application of an unconstitutional law, in connection with an appeal filed against that decision. In accordance with section 62a paragraph 1 first sentence of the Constitutional Court Act (*Verfassungsgerichtshofgesetz*, *VfGG*), a person being a party to a case decided by an ordinary court at first instance who claims infringement of their rights by the application of an unconstitutional law can file an application for the law to be found unconstitutional. 22

1.2. The present application was brought in connection with a complaint against the decision of the Klagenfurt Regional Court of 4 November 2021 dismissing an 23

objection on grounds of violation of a right pursuant to section 106 Code of Criminal Procedure.

In criminal investigation proceedings, a legal matter can be regarded as "decided [...] at first instance" – meaning an application can be lodged by a party – only if the act concerned cannot (or can no longer) be challenged by an appeal against a judgment (conviction) handed down as a result of an indictment in the main proceedings (*VfSlg. 20.001/2015*; *VfGH 7.10.2015*, *G 372/2015*; *22.9.2016, G 176/2016*). 24

That is the case here: Generally, the act of securing can be challenged by an objection on grounds of violation of a right (section 106 et seq. Code of Criminal Procedure), which can be exercised during the criminal investigation proceedings (section 91 et seq. Code of Criminal Procedure). In accordance with the case law of the Supreme Court of Justice (*OGH*), the accused can also challenge the act later on, i.e. during the main proceedings (section 210 et seq. Code of Criminal Procedure) and prevent the use of evidence produced by the securing of the device (*OGH 21.7.2009, 14 Os 47/09g* with reference to section 281 paragraph 1 subparagraph 4 Code of Criminal Procedure). However, any interference with the right to respect for private life (Article 8 ECHR) and the right to secrecy of personal data (section 1 Data Protection Act) resulting from the securing cannot be fully challenged in the latter way. This is because an appeal against a judgment given in the main proceedings can only contest the inadmissible use of evidence, but not the manner in which the evidence was taken, and especially not – as alleged by the applicant in the present case – the excessive nature of taking the evidence. The decision of the Klagenfurt Regional Court under discussion here is thus "a legal matter which has been decided at first instance". 25

1.3. Pursuant to section 62 paragraph 2 Constitutional Court Act, an application to repeal a law within the meaning of section 62a Constitutional Court Act is admissible only if the law is to be directly applied in the "pending case" or if the constitutionality of the law is – or would be in the applicant's opinion - an incidental question (*Vorfrage*) for the decision by the court in the pending case. 26

The Federal Government considers that, because the Graz Higher Court of Appeal has already given its decision on the applicant's complaint, there is no "pending 27

case" and thus one of the conditions for admissibility is not met. However, the Federal Government is in error here: From Article 140 paragraph 1 subparagraph 1 point d in combination with paragraph 8 of the Constitution it can be derived that it is not a requirement for proceedings relating to applications under Article 140 paragraph 1 subparagraph 1 point d of the Constitution that the case be pending at the time of the decision of the Constitutional Court.

1.4. As no other procedural obstacles have arisen, the main claim for repeal of section 110 paragraph 1 subparagraph 1 and paragraph 4 and section 111 paragraph 2 Code of Criminal Procedure (as amended by Federal Law Gazette I 19/2004) is admissible. Further examination of the alternative claims is therefore not required. 28

2. **On the merits** 29

In proceedings initiated upon an application filed to review the constitutionality of a law pursuant to Article 140 of the Constitution, the Constitutional Court must limit itself to deliberations on the concerns raised (cf. *VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003*). It must therefore assess only whether the provision challenged is unconstitutional on the grounds set out in the application (*VfSlg. 15.193/1998*, *16.374/2001*, *16.538/2002*, *16.929/2003*). 30

The application is well-founded. 31

2.1. The law is as follows: 32

2.1.1. In criminal investigation proceedings (section 91 et seq. Code of Criminal Procedure), section 110 paragraph 1 Code of Criminal Procedure permits the securing of items where that is deemed necessary for evidentiary reasons (subparagraph 1). 33

In accordance with section 109 subparagraph 1 point a Code of Criminal Procedure, securing (*Sicherstellung*) means (*inter alia*) the establishment of temporary power of disposition over items. In accordance with section 111 paragraph 1 Code of Criminal Procedure, the holder of such items has a (corresponding) obligation to surrender the items concerned. 34

The items which can be secured for evidentiary purposes in accordance with section 110 paragraph 1 subparagraph 1 in conjunction with section 109 subparagraph 1 point a Code of Criminal Procedure are any tangible movable objects and therefore include laptops, PCs, mobile phones (smartphones) and other electronic devices. 35

As well as allowing access to physical data storage devices, section 110 Code of Criminal Procedure also allows access to the data saved on data storage devices without the law enforcement bodies taking (physical) custody of the storage medium. This can be derived from section 110 paragraph 4 and section 111 paragraph 2 Code of Criminal Procedure, which refer to "secured information (*sichergestellte Informationen*)" (e.g. *Reindl-Krauskopf/Salimi/Stricker*, *IT-Strafrecht, 2018*, point 5.3). 36

One of the most significant differences between the securing of data storage devices and the securing of other items within the meaning of section 109 subparagraph 1 point a Code of Criminal Procedure lies not in the act of securing itself or the way it is ordered, but in the opportunity it provides to evaluate the data saved on the data storage device and the possibility to draw conclusions therefrom about the person concerned. A secured data storage device potentially contains a very large quantity of data which can, *inter alia*, be connected with and stored together with other available data (and not only data held by the law enforcement authorities). This data (including when connected with other data) can provide a comprehensive picture of the previous and current life of the person affected by the securing, which is not usually the case when other items within the meaning of section 109 subparagraph 1 point a Code of Criminal Procedure are evaluated. 37

Section 110 Code of Criminal Procedure permits law enforcement bodies access to and disposition over data storage devices which are found locally at the site of the operation. This way, custody can be taken of PCs, notebooks or smartphones and they can be searched for evidence. However, the law enforcement authorities are permitted to access not only data saved locally on the data storage device itself, but also data stored externally by, for example, accessing this data using the affected person's computer (this was also the view taken by the Federal Government in the oral hearing before the Constitutional Court; cf. Government Bill 25, supplement to the stenographic protocols of the National Council, 22nd legislative 38

period, p. 156; e.g. *Tipold/Zerbes*, *§ 111 StPO,* in: *Höpfel/Ratz* [eds.], *Wiener Kommentar zur StPO*, point 14; alternative opinion in *Reindl-Krauskopf/Salimi/Stricker*, *IT-Strafrecht,* 2018, point 5.11). This can relate to data saved on a network or some other external storage medium (e.g. in the cloud).

The law does not set out any substantive or procedural rules specifying how the law enforcement authorities should evaluate data saved (locally or externally) on a data storage device; it is therefore entirely up to the investigating authorities themselves to determine how they proceed. 39

If data saved (locally or externally) on a data storage device is encrypted or access to that data is protected, the investigating authorities are permitted to decrypt the data or disable the protection (cf. e.g. *Reindl-Krauskopf/Salimi/Stricker*, *IT-Strafrecht*, 2018, paragraph 5.7 with further references). 40

The investigating authorities are only permitted to access data that is saved on the data storage device locally or externally at the time the device is secured. The are not permitted to access (or continue to access) content saved to and stored on the device after that time; this is not covered by the power to secure items defined in section 110 paragraph 1 subparagraph 1 Code of Criminal Procedure (cf. *Tipold/Zerbes*, *§ 111 StPO*, in: Fuchs/Ratz [eds.], *Wiener Kommentar zur StPO*, rdb.at, version dated 1 March 2021, point 17/2). 41

In accordance with section 111 paragraph 2 Code of Criminal Procedure, any person is required to grant access to the information saved (locally or externally) on a data storage device and, upon request, must issue or produce an electronic data storage device in a commonly used file format. They must also acquiesce to the making of backup copies of the information saved (section 111 paragraph 2 Code of Criminal Procedure; cf. *OGH 11.9.2018, 14 Os 51/18h*). In general, section 111 paragraph 2 Code of Criminal Procedure also includes an obligation to disclose passwords and other access codes which are needed to retrieve the data. However, this does not apply to accused persons and witnesses who have a right to silence (e.g. *Reindl-Krauskopf/Salimi/Stricker*, *IT-Strafrecht*, 2018, point 5.9). 42

2.1.2. As a measure undertaken in the course of investigation proceedings, an item such as a data storage device can be secured (and evaluated) in the case of 43

mere reasonable suspicion; a strong suspicion (*dringender Verdacht*) is not required. A reasonable suspicion exists if there are specific indications giving reason to believe that a criminal offence has been committed (section 1 paragraphs 2 and 3 Code of Criminal Procedure).

2.1.3. According to the law, the criminal offence is not required to be of a particular seriousness (or encompass any aggravating elements) for the law enforcement authorities to be permitted to secure and (subsequently) evaluate the evidence; thus the only requirement is that there be specific indications giving reason to believe that a criminal offence (of any type) has been committed. 44

2.1.4. As it is a temporary measure, the securing of items – unlike seizure (section 115 paragraphs 1 and 2 Code of Criminal Procedure) – does not need to be approved by a judge; it must simply be ordered by the prosecution authority and executed by the criminal investigation authority (section 110 paragraph 2 Code of Criminal Procedure). In exceptional cases, i.e. subject to the conditions provided for in section 110 paragraph 3 Code of Criminal Procedure, the criminal investigation authority can also secure items of its own motion (section 109 subparagraph 1 point a Code of Criminal Procedure). 45

2.1.5. Like every other measure carried out in the course of investigation proceedings, securing of items and evaluation thereof are subject to the principle of proportionality provided for in section 5 paragraphs 1 and 2 Code of Criminal Procedure. Section 110 paragraph 4 Code of Criminal Procedure provides in more detail how this general principle of proportionality is to be construed, stipulating in particular that items must not be secured for evidentiary reasons pursuant to section 110 paragraph 1 subparagraph 1 Code of Criminal Procedure and secured items must be released at the request of the person concerned, if and as soon as evidentiary requirements can be met through visual, audio or other recordings or by making copies of written records or electronically processed data, and if it is not expected that the secured items themselves or the original versions of the secured information will be viewed during the trial. 46

2.1.6. In addition to items held by the accused, items in the possession of (non-suspect) third parties may also be secured (e.g. *Tipold/Zerbes*, *§ 110 StPO*, in: *Höpfel/Ratz* [eds.], *Wiener Kommentar zur StPO*, point 2); all that is required is a 47

reasonable suspicion within the meaning of section 1 paragraph 3 Code of Criminal Procedure against some (other) person and that the item in possession of the (non-suspect) third party constitutes relevant evidence in the criminal (investigation) proceedings (e.g. *Tipold/Zerbes*, *Vor §§ 110-115 StPO*, in: *Höpfel/Ratz* [eds.], *Wiener Kommentar zur StPO*, point 7).

2.1.7. Without prejudice to any remedy against the order to secure items or the evaluation of data found on the secured items (objection on grounds of violation of a right pursuant to section 106 Code of Criminal Procedure), the person affected by the securing of an item has the right to request a decision by the court to lift or continue the securing pursuant to section 115 Code of Criminal Procedure (section 111 paragraph 4 Code of Criminal Procedure). 48

Under section 75 Code of Criminal Procedure, the person concerned can also request the rectification, erasure or completion of personal data that is inaccurate or incomplete or that was collected contrary to the provisions of the Code of Criminal Procedure 1975 (cf. *OGH 13.10.2020, 11 Os 56/20z; 1.6.2021, 14 Os 35/21k*). 49

2.2. Regarding the concerns related to section 1 Data Protection Act and Article 8 ECHR 50

2.2.1. The applicant's main concern is that the securing of data storage devices such as smartphones constitutes an interference of particular intensity, and that the conditions under which it is permitted are insufficiently stringent. 51

In particular, the securing of a mobile phone (smartphone) and the data saved on it provides deep insights into the life and private sphere of the person concerned. Despite this, all that is required for a mobile phone to be secured is an order by the prosecution authority in the course of criminal investigation proceedings, and in turn all that is required to initiate such proceedings is a reasonable suspicion. In light of the severity of the interference with the fundamental right to data protection and to private and family life caused by the securing of items, the standard applied is contradictory: It is inconsistent that the law does not require the securing of items to be ordered by a court, while it does so for other measures which are less or similarly intrusive on fundamental rights (such as disclosure of bank 52

data under section 116 Code of Criminal Procedure or house searches under section 120 Code of Criminal Procedure). The powers granted to law enforcement authorities permit unlimited interference with private life in terms of the time period and content concerned because the legislator has not provided for (adequate) determinants. Furthermore, the law does not specify any conditions regarding the severity of the criminal offence that the suspect is alleged to have committed.

In response to this concern, the Federal Government argues, in summary, that the securing of data (storage devices) is subject to the principle of proportionality, that only information which is relevant for criminal justice purposes can be examined, and that there is adequate legal protection for the person concerned. Data is evaluated for criminal prosecution purposes only and requires to be ordered. Information which is not relevant for criminal justice purposes must be deleted and is not allowed to be put on file. A reasonable suspicion within the meaning of section 1 paragraph 3 Code of Criminal Procedure is required before items can be secured and grounds for securing the items specified must be given. The securing of items is a temporary measure only; seizure (as a measure of longer duration) is subject to judicial approval. In addition, the law enforcement authorities must also observe the general principle of proportionality pursuant to section 5 Code of Criminal Procedure when securing and evaluating items. Finally, section 115 and section 106 Code of Criminal Procedure also provide adequate legal protection to persons affected by the securing of items or seizure. 53

2.2.2. Apart from Article 8 ECHR, federal constitutional law also provides for a specific fundamental right to data protection. 54

2.2.2.1. The fundamental right to data protection pursuant to section 1 paragraph 1 of the Data Protection Act guarantees every person the right to secrecy of the personal data concerning that person, especially with regard to the respect for their private and family life, insofar as that person has an interest in such secrecy which requires protection. This claim to secrecy of personal data requiring protection is not only intended to prevent the disclosure of data which has been collected, but also prohibits data subjects from being unlawfully obliged to disclose data. This protection also applies if the obligation to disclose is imposed not on the 55

data subject personally, but on a third party with disposal over protected data relating to the data subject (*VfSlg. 12.228/1989, 12.880/1991, 16.369/2001, 19.673/2012*).

56 To that end, section 1 paragraph 2 Data Protection Act contains a substantive reservation which draws the limits for interference with this fundamental right more narrowly than Article 8 paragraph 2 ECHR (*VfSlg. 19.892/2014*): Accordingly, besides the use of personal data in the vital interest of the data subject or with the data subject's consent, restrictions to the right to secrecy are permitted only in order to safeguard overriding legitimate interests of another person, namely in the case of interference by a public authority only on the basis of laws which are necessary for the reasons specified in Article 8 paragraph 2 ECHR and which set out sufficiently precisely – i.e. in a manner foreseeable for everybody - the circumstances under which the gathering or use of personal data is permitted for the performance of specific administrative functions (cf. *VfSlg. 16.369/2001, 18.146/2007, 18.643/2008, 18.963/2009, 19.886/2014, 19.892/2014, 20.213/2017*). Thus in accordance with section 1 paragraph 2 Data Protection Act, the legislator must stipulate a subject-specific provision specifying and restricting cases in which interference with the fundamental right to data protection is permitted (*VfSlg. 18.643/2008, 19.886/2014, 20.213/2017*).

57 Laws providing for the use of data which, due to its nature, requires particular protection may, as section 1 paragraph 2 Data Protection Act (going beyond Article 8 paragraph 2 ECHR) further states, allow such use only in order to safeguard substantial public interests and, at the same time, must provide for adequate safeguards for the protection of the data subjects' secrecy interests.

58 2.2.2.2. Even in the case of permitted restrictions, a fundamental right may only be interfered with using the least intrusive of all effective methods. According to the case law of the Constitutional Court, it follows from this that the proportionality of the interference in the fundamental right to data protection under section 1 Data Protection Act must be measured against a more rigorous standard than that required by Article 8 ECHR (*VfSlg. 16.369/2001, 18.643/2008, 19.892/2014, 20.356/2019*). In accordance with Article 8 ECHR, all people have the right to respect for their private and family life, their home and their correspondence. Interference by a public authority with the exercise of this right is permitted

only if it is in accordance with the law and constitutes a measure which is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

59 The collection and storage of data relating to specific persons by the security authorities may constitute an interference with this constitutionally guaranteed right to respect for private and family life (ECtHR, 26 March 1987, *Leander against Sweden*, appl. no. 9248/81 [paragraph 47 et seq.]; 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05 [paragraph 43 et seq.]), particularly if such acts are carried out systematically or covertly (cf. ECtHR, 6 September 1978, *Klass and Others v. Germany*, appl. no. 5029/71 [paragraph 41]; 24 April 1990, *Kruslin v. France*, appl. no. 11801/85 [paragraph 26]; 6 June 2006, *Segerstedt-Wiberg and Others v. Sweden*, appl. no. 62332/00 [paragraphs 72-73]; 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05 [paragraph 46].

60 According to the case law of the European Court of Human Rights, the protection of personal data is of fundamental importance to a person's enjoyment of their right to respect for private and family life, as guaranteed by Article 8 of the ECHR. The domestic law must provide for appropriate safeguards to prevent any such use of personal data that may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, and in particular when such data is used for police purposes. The domestic law is required to specifically ensure that such data is relevant and not excessive in relation to the purposes for which it is stored and that it is preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which this data is stored (cf. ECtHR, 4 December 2008 [GC], *S. and Marper v. the United Kingdom*, appl. no. 30562/04, [particularly paragraph 103]).

61 2.2.3. Two of the provisions challenged in the present application, i.e. section 110 paragraph 1 subparagraph 1 and section 111 paragraph 2 Code of Criminal Procedure, grant law enforcement authorities the power to secure data storage devices, and in a further step, the power to evaluate, store and process data including (sen-

sitive) personal data within the meaning of section 1 Data Protection Act and Article 8 ECHR. The power to secure data storage devices thus interferes with the right to data protection under section 1 Data Protection Act and the right to respect for private and family life under Article 8 ECHR of both suspects and (non-suspect) third parties.

It is clear to the Constitutional Court that the objective pursued in section 110 et seq. Code of Criminal Procedure, i.e. that of prosecution of criminal offences by way of securing (access and evaluation) of evidence, which includes data storage devices, is a legitimate aim within the meaning of section 1 paragraph 2 Data Protection Act and Article 8 paragraph 2 ECHR. The powers granted to the law enforcement authorities in section 110 et seq. Code of Criminal Procedure are also appropriate in general to achieve this (legitimate) aim. 62

2.2.4. A further condition that must be met for an interference with the fundamental right to data protection under section 1 Data Protection Act and the right to respect for private and family life under Article 8 ECHR to be deemed proportionate and thus legitimate is that the severity of the specific interference must not exceed the gravity and importance of the aims pursued by the interference (e.g. *VfSlg. 19.738/2013, 19.892/2014*; ECtHR, 4 December 2008 [GC], *S. and Marper v. the United Kingdom*, appl. no. 30562/04, [paragraph 101]). With regard to data requiring particular protection, section 1 paragraph 2 second sentence Data Protection Act imposes a further limitation on interference, stipulating that such data may only be used where necessary to safeguard substantial public interests and that the individual laws must provide for adequate safeguards for the protection of the data subjects' secrecy interests. 63

The Constitutional Court holds the view that the provisions challenged do not satisfy these requirements. 64

2.2.5. As also concluded in the discussion during the oral hearing before the Constitutional Court, the securing of data storage devices and in particular the evaluation of such devices in accordance with section 110 paragraph 1 subparagraph 1 and section 111 paragraph 2 Code of Criminal Procedure is not comparable with the securing (access and evaluation) of other (tangible, movable) items: 65

Access to potentially all of the data held on a data storage device does not merely give law enforcement authorities a momentary snapshot of the behaviour of the suspect or the person affected by a coercive measure (as defined in section 48 paragraph 1 subparagraphs 1 and 4 Code of Criminal Procedure). Data saved (locally or externally) on a secured data storage device such as a laptop, PC or smartphone, which is potentially accessible to law enforcement authorities when they evaluate the device, also gives those authorities comprehensive insight into substantial parts of the previous and current life of the person concerned. The law enforcement authorities are given the power to investigate and save all content and connection data relating to all communications (possibly including those which have already been erased), and to connect, synchronize and systematize it with data available elsewhere, especially on the internet or in databases. In this way, they can build comprehensive personality and movement profiles revealing detailed information about the behaviour, personality and attitudes of those concerned. The connection data recorded on the data storage device also enable them to make assumptions regarding the content of communications because this data shows whether and with whom the person concerned has communicated, and when, how often and by what means communication took place (cf. *VfSlg. 19.892/2014*; CJEU, 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and others, paragraph 27; CJEU, 13 May 2014, *Google Spain and Google*, C-131/12, paragraph 80 et seq.; CJEU, 21 December 2016, *Tele2 Sverige AB*, C-203/15, paragraph 98-99). 66

Apart from the affected person's communications, law enforcement authorities potentially also have access to all other data, including sensitive and other personal data, saved (locally or externally) on the data storage device. This data can include photos, videos, location data, search histories or health data which, taken together and alongside the saved communication content referred to above, enable law enforcement authorities to build a complete profile of the person concerned. 67

A further feature of the evaluation of data saved (locally or externally) on a data storage device is that, if certain data types or quantities relating to the person concerned are available, predictive analysis can be used to draw conclusions about the behaviour, preferences, attitudes and thus the personality generally of the 68

person concerned, even if no specific data regarding any of these aspects is held on the secured device.

In addition, it is important to note that this potentially comprehensive insight by the law enforcement authorities into data saved (locally or externally) on a secured data storage device relates not only to data storage devices in the custody of an individual suspect in specific criminal proceedings, but also applies to devices held by (non-suspect) third parties. 69

In view of the quantity of data normally present on data storage devices (such as PCs, notebooks and smartphones), the content of that data and the potential for it to be connected and synchronized with other data and under certain circumstances the potential for deleted data to be restored, the securing of a data storage device and in particular the evaluation of the data saved (locally or externally) on that device cannot be compared with the securing and evaluation of other items within the meaning of section 109 subparagraph 1 point a Code of Criminal Procedure. The securing (access and evaluation) of data storage devices and the data saved on them (locally or externally) raises questions of constitutional law beyond this. 70

2.2.6. The Constitutional Court takes the view that the investigative measure of securing data storage devices pursuant to section 110 paragraph 1 subparagraph 1 and section 111 Code of Criminal Procedure constitutes an interference of a particular intensity for the following reasons: 71

Firstly, the law enforcement authorities can take the measures provided for in section 110 paragraph 1 subparagraph 1 and section 111 Code of Criminal Procedure (securing of data storage devices and evaluation of the data saved on them) on the basis of mere reasonable suspicion within the meaning of section 1 paragraph 3 Code of Criminal Procedure. Secondly, the suspicion can relate to any criminal offence and need not concern an offence of a particular seriousness. Thirdly, these measures may be directed not only against a suspect but also against a (non-suspect) third party. Fourthly, the law enforcement authorities potentially have access to all data – including sensitive data, which are or were saved (locally or externally) on the secured data storage device – and thus to all content and connection data on that device. The securing (access and evaluation) of data 72

saved on data storage devices such as PCs, notebooks and mobile phones enable the law enforcement authorities to access information relating to every part of the life of the person concerned. As it is (technically) possible to reconstruct deleted data, the insights which law enforcement authorities are able to gain by securing a data storage device extends (potentially without limitation) to data which was held on the device in the past. The investigative measure not only affects persons who are reasonably suspected of having committed a criminal offence, but also affects every person whose data is held on the secured data storage device.

It can therefore be derived from all of the above that, as regards the intensity of the interference, the powers granted to the law enforcement authorities under section 110 paragraph 1 subparagraph 1 and section 111 Code of Criminal Procedure pose a particularly serious threat to the sphere of fundamental rights protected by section 1 paragraph 1 Data Protection Act in conjunction with Article 8 paragraph 1 ECHR. 73

2.2.7. Reference is made here to the case law of the European Court of Human Rights, which has repeatedly emphasized the risk that systems of (secret) surveillance may undermine or even destroy democracy under the cloak of defending it. With this in mind, the European Court of Human Rights, when assessing such measures, considers the degree of determination of the relevant law, the nature, scope and duration of the measure, the authorities competent to permit, carry out and supervise the measure, available legal protection and guarantees against abuse in relation to one another (cf. ECtHR, 6 September 1978, *Klass v. Germany*, appl. 5029/71, [paragraph 49-50]; also e.g. ECtHR, 4 December 2015 [GC], *Zakharov v. Russia*, appl. no. 47.143/06, [paragraph 232-33], and 12 January 2016, *Szabó and Vissy v. Hungary*, appl. no. 37.138/14, [paragraphs 57 and 77 with further references]). 74

This securing (access and evaluation) of data storage devices is not a “secret” or “undercover” investigative measure, as the person concerned is aware that the law enforcement authorities have secured their data storage device. In the view of the Constitutional Court, however, it cannot be regarded as a truly “open” measure either (cf. *Reindl-Krauskopf/Salimi/Stricker*, op. cit., point 5.13; *Tipold/Zerbes*, *§ 111 StPO*, in: *Höpfel/Ratz* [eds.], *Wiener Kommentar zur StPO,* rdb.at, version dated 1 March 2021, point 17), as it is not evident to the person 75

concerned how the data saved (externally or locally) on the data storage device will be evaluated (e.g. whether deleted data is restored, whether the data is connected with other data, etc.).

2.2.8. The Constitutional Court recognizes that the rapid expansion of the use of "new" communication technologies (e.g. mobile telephony, email, exchanging of information via the world wide web, etc.) has posed and will continue to pose particular challenges for the state in a number of respects – not least in combatting crime, which the securing of data storage devices is intended to serve. The Constitutional Court gives due regard to this changed environment for police investigations in its case law (cf. e.g. VfSlg. 16.149/2001, 16.150/2001, 18.830/2009, 18.831/2009, 19.657/2012). However, it is important to recognize that the greater investigative possibilities afforded by state-of-the-art technical tools that are available to law enforcement authorities also mean that the dangers posed thereby to human liberty must be countered in a manner that is appropriate (*VfSlg. 19.892/2014, 20.356/2019*). 76

2.2.9. For situations where the legislator has granted the law enforcement authorities extensive powers of intervention, section 1 Data Protection Act in conjunction with Article 8 ECHR require effective legal protection to safeguard that the conditions for both securing and evaluation of data saved on a secured data storage device are met effectively and the misuse of powers is prevented. This applies all the more in the present case, where (some of) the data processed is regarded as requiring particular protection within the meaning of section 1 paragraph 2 second sentence Data Protection Act (for example health data). 77

As previously stated by the Constitutional Court in *VfSlg. 19.892/2014,* review by a judge is necessary for effective legal protection because – in view of the extensive powers and particularly intrusive interference granted to the law enforcement authorities in the present case, and, consequently, the measures necessary to prevent abuse thereof – effective protection of fundamental rights can only be guaranteed by way of judicial control. 78

In view of the extensive access granted to the law enforcement authorities under section 110 paragraph 1 subparagraph 1 and section 111 paragraph 2 Code of 79

Criminal Procedure, the court must, when approving the securing and (subsequent) evaluation of a data storage device, determine the categories and content of data allowed to be evaluated, the period to be covered by the data evaluation as well as the underlying (investigative) purposes.

2.2.9.1. Specifically in relation to the securing of data storage devices and (subsequent) evaluation of the data saved on them, the Constitutional Court cannot discern any objective justification for the fact that approval by the court is required only for the seizure of items (which are usually secured previously) within the meaning of section 109 subparagraph 1 point a Code of Criminal Procedure, but not for the securing itself (cf. section 115 paragraph 2 Code of Criminal Procedure). 80

Once the data saved on a secured data storage device has been evaluated (which is generally admissible), seizure of the device under section 115 Code of Criminal Procedure does not normally offer any "added value" because, as a rule, the investigative measures of importance to the law enforcement authorities are taking a copy of all of the data saved (locally and externally) on the data storage device and then evaluating that data. By evaluating the data saved on the secured data storage device and copying or saving or otherwise storing the data found on it, the law enforcement authorities effectively seize the data without having to comply with the provisions set out in section 115 paragraph 2 Code of Criminal Procedure. 81

2.2.9.2. Accordingly, the power of investigation granted to the prosecution authority (and the criminal investigation authority) under section 110 paragraph 1 subparagraph 1 and section 111 paragraph 2 Code of Criminal Procedure without any requirement for prior approval by the court violates section 1 paragraph 2 Data Protection Act in conjunction with Article 8 paragraph 2 ECHR (cf. also *VfSlg. 19.892/2014*). 82

2.2.10. The provisions challenged additionally violate section 1 paragraph 2 of the Data Protection Act in conjunction with Article 8 paragraph 2 ECHR for a further reason. The Code of Criminal Procedure 1975 does not provide adequate legal protection during the investigation proceedings and subsequent (main) proceedings for persons affected by the securing (access and evaluation) of data storage devices. 83

2.2.10.1. In both its written observations and its arguments during the oral hearing before the Constitutional Court, the Federal Government takes the view that, as regards the securing and evaluation of data storage devices, persons affected thereby have sufficient legal remedies available to them: 84

Those affected can ask the court to lift or continue the securing under section 110 paragraph 4 Code of Criminal Procedure. The person affected by securing is also entitled to bring an objection on grounds of violation of a right against the order of the prosecution authority before the regional court (section 106 Code of Criminal Procedure) and a complaint against that court's decision before the higher court of appeal (section 107 paragraph 3 Code of Criminal Procedure), the Federal Government argues. In addition, a person affected by a coercive measure as defined in section 75 Code of Criminal Procedure can request the erasure of personal data that was collected in contravention of the Code of Criminal Procedure 1975. That includes any personal data which is not of use for the investigation of criminal offences (cf. *OGH 13.10.2020, 11 Os 56/20z; 1.6.2021, 14 Os 35/21k*). 85

2.2.10.2. Contrary to this, the Constitutional Court takes the view that the legal protection is not sufficient: The legal protection provided against the extensive powers of investigation granted to the law enforcement authorities under section 110 paragraph 1 subparagraph 1 and section 111 paragraph 2 Code of Criminal Procedure is not adequate in light of the requirements enshrined in section 1 Data Protection Act in conjunction with Article 8 ECHR. 86

Pursuant to Section 110 paragraph 4 Code of Criminal Procedure, a person affected by the securing of items can request that the securing be lifted subject to the conditions set out in that provision. However, once a data storage device has been secured and the data saved on it has been evaluated, no legal protection is provided regarding the question of whether the securing was lawfully ordered by the prosecution authority and lawfully executed by the criminal investigation authority. 87

Section 106 Code of Criminal Procedure, which accords any person affected by an investigative measure carried out by the prosecution authority the right to bring an objection on grounds of violation of a right, and section 75 Code of Criminal Procedure, which grants any person affected by a coercive measure the right to 88

request the immediate rectification, completion or erasure of personal data that is inaccurate or incomplete or that was obtained in contravention of the provisions of this Code, provide appropriate legal protection to some extent against the unlawful securing of data storage devices and evaluation of the data saved on them. However, the above provisions do not fully ensure legal protection because in many cases the person concerned will not learn of possible violations of their rights, and more generally will not be aware of how the prosecution authority (and criminal investigation authority) actually proceed when evaluating the data saved on their data storage device. This impacts heavily on the ability of suspects to defend themselves during the investigation proceedings (and in the subsequent main proceedings), as well as on persons who are not directly involved in the criminal investigation (non-suspect third parties).

2.2.10.3. The Constitutional Court also takes the view that, in light of section 1 Data Protection Act and Article 8 ECHR, the requirement that the authorities in charge of investigation proceedings must observe the general principle of proportionality set out in section 5 Code of Criminal Procedure is not sufficient. 89

As outlined above, for an item to be secured for evidentiary reasons, as for any other investigative measure, a reasonable suspicion must be present, i.e. there must be specific indications that a criminal offence has been committed (section 1 paragraphs 2 and 3 Code of Criminal Procedure). The item to be secured must also be suitable for being used as evidence of that offence, meaning that the item must be expected to serve the investigation of the offence (cf. *Tipold/Zerbes*, *§ 110 StPO*, in: *Fuchs/Ratz* [eds.], *Wiener Kommentar zur StPO*, rdb.at, version dated 1 March 2021, point 5). In accordance with section 3 paragraph 1 Code of Criminal Procedure, law enforcement authorities are required to act objectively and must investigate incriminating and mitigating circumstances with equal care. 90

It is for the law enforcement authorities – duly taking into account the principle of proportionality of section 5 Code of Criminal Procedure – to keep to a minimum any interference with the fundamental rights in each case (see *OGH 28.7.2020, 11 Os 51/20i; 13.10.2020, 11 Os 56/20z*). Consequently, data storage devices may be secured only if the same aim cannot be achieved using other less intrusive measures (section 5 paragraph 2 first sentence Code of Criminal Procedure). Ad- 91

ditionally, the infringement of legally protected interests resulting from the securing (access and subsequent evaluation) must be reasonably proportionate to the gravity of the presumed criminal offence (section 5 paragraph 1 second sentence Code of Criminal Procedure).

In view of the great number and type of technical tools and legal powers available to law enforcement authorities for evaluating data saved (locally or externally) on a data storage device, which permit serious interference with the fundamental right to data protection under section 1 Data Protection Act and the fundamental right to private and family life under Article 8 ECHR, the Constitutional Court considers that it is not sufficient for the legislator to impose the obligation to observe the general principle of proportionality in section 5 Code of Criminal Procedure on the law enforcement authorities. 92

This is due, firstly, to the fact that compliance with the principle of proportionality consists only in an assessment as to whether or not an item should be secured. As a rule, this assessment considers only whether a specific piece of evidence can be obtained in a manner other than by securing the item within the meaning of section 109 subparagraph 1 point a Code of Criminal Procedure. If it cannot, the item in question must be secured and the proportionality review ends there. 93

Secondly, as the law grants the law enforcement authorities powers of investigation that are comprehensive and extensive enough to permit serious interference with the fundamental rights of those affected, it must also specify the main limits to permissibility of the various investigative steps concerned. 94

2.2.10.4. As discussed in 2.2.5. and 2.2.7 above, the securing and evaluation of data storage devices constitute comprehensive and extensive investigatory powers because it is (technically) possible to access and evaluate all the data saved (locally or externally) on a device. Furthermore, it is possible to access external storage media (e.g. network systems or cloud storage) from a data storage device which has been secured. All this means, firstly, that the law enforcement authorities can access data and information dating back many years. Secondly, the huge amount and type of data saved (locally or externally) on a data storage device allows the law enforcement authorities to build an extensive profile of the affected 95

person's behaviour and movements. Thirdly, the filters used by the law enforcement authorities to build this profile, as well as filters used generally (in the form of algorithms or search terms, for example) have implications for the result of the evaluation. Fourthly, the law enforcement authorities are at liberty to connect data stored on the data storage device with other data available to them. In addition to this – and this was also shown in the oral hearing before the Constitutional Court – any changes made to the data by the body carrying out the evaluation cannot (with currently available technology) be specifically identified after the event; it is only possible to determine that changes have been made but the actual changes cannot be assessed.

2.2.10.5. In light of the technical tools and legal powers available to the law enforcement authorities as described above, judicial review (which the Constitutional Court regards as necessary, see 2.2.9. above) that takes place only at the beginning of the process, i.e. when the order to secure (access and evaluate) a data storage device is approved by a judge, does not afford a person affected by the securing of data storage devices sufficient legal protection as required by section 1 of the Data Protection Act and Article 8 ECHR (cf. also *VfSlg. 20.356/2019*). 96

When defining the legal requirements for the investigative measure of the securing of data storage devices and the evaluation of data saved on them (locally or externally), the legislator must weigh the public interest in the prosecution and investigation of criminal offences on the one hand against the protected fundamental right of persons affected by securing, especially the right to protection of their secrecy interests and the right to protection of their private sphere and family life under section 1 Data Protection Act and Article 8 ECHR on the other, and strike an appropriate balance between them. 97

The constitutional requirements for striking this balance with regard to the securing of data storage devices and the evaluation of data saved on them (locally or externally) for the purposes of administration of the criminal justice system vary depending on the intensity of the interference resulting from the specific legislation in place. When conducting this proportionality review, the legislator must take account of the following aspects in particular: 98

It may make a difference if the law permits data storage devices to be secured and the data saved on them (locally or externally) to be evaluated in cases of reasonable suspicion of a criminal offence regardless of the seriousness of the offence, the legal interest protected or the data storage devices typically used in the commission of crime (cybercrime), or if the law provides for securing and evaluation for certain offences only. 99

Another relevant factor in a constitutional assessment of the investigative measure of the securing of data storage devices is the question of whether the legislator has put in place safeguards limiting the evaluation of a secured data storage device to the minimum necessary and ensuring that, organizationally and technically, such evaluation is conducted in a manner which exposes the procedure and any analytical tools used to scrutiny and verification (cf. also *VfSlg. 19.592/2011* [point III.2.4.1.]). 100

The legislator must ensure that persons affected by the securing of a data storage device and the evaluation of data saved (locally or externally) on it receive (or are able to receive) in a suitable manner the information required to safeguard their rights during the investigation proceedings and any subsequent main proceedings. 101

Moreover, given the nature and volume of data that is accessible on a secured data storage device and that can be evaluated by the law enforcement bodies, it may be significant that the legislator – weighing the securing and evaluation of data against the conflicting interest in administration of the criminal justice system – provides for effective mechanisms of independent review to verify whether law enforcement authorities acted within the limits of the judicial approval and statutory safeguards and whether the rights of the affected persons to protection of their private sphere and secrecy interests were appropriately safeguarded during the process of evaluation or processing of the secured data storage devices, even if the persons concerned are not present when the device is evaluated. 102

2.2.10.6 Since the provisions challenged (section 110 paragraph 1 subparagraph 1 and paragraph 4 as well as section 111 Code of Criminal Procedure) do not meet the requirements listed above, they are contrary to section 1 Data Protection Act and Article 8 ECHR for these reasons too. 103

2.3. Against this background, it is not necessary to comment on the applicant's concerns raised in connection with the principle of equal treatment under Article 2 of the Basic State Law (*StGG*) and Article 7 of the Constitution (*B-VG*). 104

V. Result

1. Section 110 paragraph 1 subparagraph 1 and paragraph 4 as well as section 111 paragraph 2 of the Code of Criminal Procedure are repealed as unconstitutional. 105

The date when the repealed provisions will cease to be in force is set in accordance with Article 140 paragraph 5 third and fourth sentences of the Constitution. The ruling that previous legal provisions shall not re-enter into force is founded on Article 140 paragraph 6 of the Constitution. 106

2. The obligation of the Federal Chancellor to publish the repeal and the associated rulings without delay derives from Article 140 paragraph 5 first sentence of the Constitution and section 64 paragraph 2 Constitutional Court Act in conjunction with section 3 subparagraph 3 of the Federal Act on the Federal Law Gazette (*Bundesgesetzblattgesetz, BGBlG*). 107

Vienna, 14 December 2023
The President:
GRABENWARTER

Recording clerk:
MÜLLNER