https://doi.org/10.22364/iscflul.10.20

Raimondas Andrijauskas, *Master of Law (PhD student)*
Mykolas Romeris University, Lithuania

IN SEARCH OF A BALANCE: PERSONAL DATA PROTECTION DURING EXTRAORDINARY SITUATIONS

Key words: personal data protection, extraordinary situations, proportionality principle

Summary

The Charter of Fundamental Rights of the European Union recognises the protection of personal data as a fundamental right (Article 8). Recent extraordinary situations in Europe – including the migration and refugee crisis, terrorist attacks, the COVID-19 pandemic, and the war in Ukraine – have prompted EU Member States to adopt emergency measures relying extensively on digital technologies, such as real-time facial recognition systems, contact-tracing and location-tracking applications, and large-scale health data processing mechanisms.

While these measures are frequently justified by urgent public-interest objectives, they raise serious concerns regarding their legality, necessity, and proportionality. Emergency responses are often characterised by accelerated decision-making, limited ex ante impact assessments, and reduced public scrutiny, increasing the risk that temporary measures may outlast the extraordinary situations that justified their adoption. As a result, such practices may lead to disproportionate interferences with the fundamental right to personal data protection, particularly affecting vulnerable or marginalised groups.

This research examines the relationship between extraordinary legal regimes and personal data protection within EU Member States. It addresses the challenges of assessing the proportionality of emergency data processing measures, noting that systematic judicial analysis in this area remains limited. By analysing decisions of constitutional and administrative courts concerning extraordinary data processing measures challenged by individuals or political actors, the study identifies emerging judicial standards for reviewing governmental actions that restrict the right to personal data protection.

The research contributes to both academic discourse and practical governance by proposing a framework for safeguarding core data-protection principles during crises. By synthesising judicial reasoning and best practices derived from case law, it offers guidance for ensuring that emergency measures remain lawful, proportionate, time-limited, and respectful of the essence of fundamental rights.

Introduction

The protection of personal data has gradually evolved into a core element of European constitutionalism. Although the European Economic Community was originally conceived as a project of economic integration, the expansion of European Union (EU or Union) competences and the increasing impact of EU law on individuals revealed the necessity of recognising and safeguarding fundamental rights within the Union's legal order. This evolution culminated in the adoption of the Charter of Fundamental Rights of the European Union[1] (the Charter), which acquired binding legal force with the entry into force of the Treaty of Lisbon[2] in 2009.

The Treaty of Lisbon introduced major changes to the EU's legal architecture, most notably by elevating the Charter to constitutional status.[3] Among the rights enshrined in the Charter, the right to the protection of personal data occupies a distinctive position. Article 8 explicitly recognises data protection as an autonomous fundamental right, closely linked to, yet distinct from, the right to respect for private and family life. The constitutionalisation of data protection reflects the growing importance of information processing in modern societies and the corresponding risks posed by technological developments.

This constitutional commitment has been repeatedly tested during extraordinary situations. Successive crises – including migration and refugee movements, terrorist attacks, the COVID-19 pandemic, and the war in Ukraine – have prompted Member States to invoke emergency powers and to deploy digital technologies for surveillance, monitoring, and control. Although such measures are frequently justified by urgent public-interest objectives, they intensify the tension between effective crisis management and the protection of fundamental rights. Despite their effectiveness in addressing crises, these tools often escape ordinary legal scrutiny and lack systematic evaluation or sunset clauses, raising concerns about their long-term effects on privacy and data protection.[4] What is at stake is not merely administrative discretion but the constitutional integrity of liberal democracy within EU Member States. As Bruce Ackerman observed, modern democracies increasingly deploy emergency powers not solely to repel threats but to reassure citizens of the state's capacity to act.[5] This "reassurance function" alters the constitutional balance: governments feel compelled to display visible

---

1 Charter of Fundamental Rights of the European Union. Proclaimed in Nice on 07.12.2000 [in the wording of 01.12.2009].

2 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. Signed in Lisbon on 13 December 2007 [in the wording of 1 December 2009].

3 European Union Agency for Fundamental Rights. Handbook on European Data Protection Law – 2018 edition. Vienna: European Union Agency for Fundamental Rights (FRA), 2018, pp. 28–29.

4 European Parliament. The Impact of Covid-19 Measures on Democracy, the Rule of Law and Fundamental Rights in the EU, pp. 2–5. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651343/IPOL_BRI(2020)651343_EN.pdf [last viewed 03.11.2025].

5 Ackerman B. The Emergency Constitution. Yale Law Journal, Vol. 113, No. 5, 2004, p. 1037. https://doi.org/10.2307/4135710

control – often through technological or surveillance measures – even when the necessity for such control is ambiguous or temporary.

Against this background, the central question addressed in this research is how the right to personal data protection can be preserved during extraordinary situations without undermining the capacity of states to respond effectively to crises. By examining constitutional principles, EU legal standards, and judicial practice, this study seeks to identify criteria for assessing the proportionality and legality of emergency data-processing measures.

1. Constitutional nature and features of extraordinary measures

European constitutional systems, deeply rooted in the Western legal tradition inherited from the ancient Roman Republic, recognise extraordinary measures as a temporary deviation from ordinary governance, permissible only under strict and clearly defined conditions. The very concept of *extraordinaria potestas* – exceptional authority granted in times of crisis – originated in Roman constitutional thought, where the dictatorship was conceived as a limited and temporary institution, activated solely to restore the normal legal order.[6]

This historical paradigm profoundly influenced later Western constitutional developments, including those of EU Member States, in which the principles of temporality, legality, proportionality, and restoration of normality continue to guide the design and application of emergency legal regimes. However, as societies and democratic governance evolved, the interpretation of these principles has become more nuanced: contemporary constitutional systems increasingly emphasise human rights safeguards, parliamentary oversight, and judicial review as integral components of lawful emergency governance, thereby adapting the ancient Roman legacy to the requirements of modern constitutional democracy.[7] European constitutional systems recognise extraordinary measures as a temporary deviation from ordinary governance, permitted under strict conditions. Their main features are, as follows:

1.1. Existence of grounds for introduction of extraordinary situation – clearly identified threat

Extraordinary legal regimes may be introduced only in the presence of a clearly defined and legally recognised threat to the constitutional order, public security, or national safety. Such measures must rest upon an explicit constitutional or statutory basis specifying the nature of the threat and the authority competent to declare the emergency. For instance, Article 144 of the Constitution of the Republic of

[6] Lintott A. The Constitution of the Roman Republic. Oxford: Oxford University Press, 1999 (reprinted 2009), pp. 96, 229.

[7] Ackerman B. A. 2004, pp. 1046–1056.

Lithuania authorises the declaration of a state of emergency in peacetime when necessary to safeguard the constitutional order or public peace.[8] Similarly, Art. 62 of the Constitution of the Republic of Latvia provides for the proclamation of a state of emergency in situations of internal insurrection or threat to the existing political system.[9] In the same vein, Art. 35 and 91 of the German Basic Law (*Grundgesetz*) empower the federal authorities to take special measures in cases of internal unrest or natural disasters.[10]

Most modern constitutions of EU Member States contain analogous provisions, reflecting a shared European constitutional tradition in which extraordinary powers are justified only by the existence of a concrete and imminent threat, and their activation is subject to strict substantive and procedural safeguards.[11]

1.2. Discretionary power to declare an extraordinary situation

Constitutions generally vest the competence to declare a state of emergency or other extraordinary legal regime in specific state authorities, most commonly the head of state, the government, or the national parliament.[12] The exercise of this discretionary power is not absolute but is constrained by the principles of separation of powers and constitutional checks and balances. Accordingly, the declaration of an extraordinary situation must comply with substantive and procedural safeguards, including the requirement of a formal legal act, parliamentary authorisation or confirmation, and, in some systems, subsequent judicial review to ensure that the declaration is both lawful and proportionate to the circumstances prompting it.

1.3. Entity granted powers to apply extraordinary measures

Once an extraordinary legal regime has been lawfully declared, specific governmental authorities are entrusted with the implementation of extraordinary measures within the scope defined by the constitution or enabling legislation. In

---

[8] The Constitution of the Republic of Lithuania. Available: https://www.lrs.lt/home/Konstitucija/Constitution.htm [last viewed 03.11.2025].

[9] The Constitution of the Republic of Latvia. Available: https://saeima.lv/en/about-saeima/work-of-the-saeima/constitution/ [last viewed 03.11.2025].

[10] Basic Law for the Federal Republic of Germany. Available: https://www.gesetze-im-internet.de/englisch_gg/ [last viewed 03.11.2025].

[11] European Parliamentary Research Service. States of Emergency in Response to the Coronavirus Crisis: Normative Response and Parliamentary Oversight in EU Member States during the First Wave of the Pandemic, EPRS Study PE 659.385, pp. 16–24. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/659385/EPRS_STU(2020)659385_EN.pdf [last viewed 03.11.2025].

[12] Bellenghi G. The European Parliament's Proposal for an EU State of Emergency Clause: A Comparative and Constitutional Analysis. Croatian Yearbook of European Law & Policy, Vol. 20, No. 1, 2024, p. 9. https://doi.org/10.3935/cyelp.20.2024.586

practice, this often has direct implications for data protection: once an emergency is declared, new data-collection or surveillance measures may be introduced without ordinary legislative scrutiny, expanding executive control over information systems.[13] Such empowerment reflects the functional necessity of ensuring an effective state response to exceptional threats; however, it simultaneously raises profound concerns regarding the principles of legality, proportionality, and oversight.

1.4. Suspension of ordinary law and limited protection of rights

Extraordinary legal regimes may entail the temporary suspension or derogation of certain provisions of ordinary law, including the limitation of individual fundamental rights. Such measures, however, must remain strictly consistent with constitutional principles and particularly with the principle of proportionality as embedded in both national constitutional traditions and EU law. While the suspension of ordinary legal norms may be justified by the imperative of addressing a grave and immediate threat, it does not authorise the abrogation of fundamental rights or the displacement of the rule of law. The European Convention on Human Rights[14] (Art. 15) and the Charter (Art. 52) establish that any such derogation must be necessary, proportionate, and preserve the essence of the protected rights.

Similarly, national constitutions often allow temporary suspension or restriction of privacy and data-protection guarantees. For example, emergency data-retention laws adopted during the COVID-19 crisis enabled authorities to track citizens' movements or health data. However, even in these circumstances, the core (essence) of fundamental rights must remain protected – a principle confirmed by the Court of Justice of the European Union (CJEU) in La Quadrature du Net (2020).[15]

1.5. Temporary nature of the extraordinary situation

A defining characteristic of any extraordinary legal regime is its inherently temporary nature. Emergency measures must be strictly time-bound, justified solely for the duration of the exceptional threat, and terminated once the conditions necessitating their adoption cease to exist. This principle reflects one of the central tenets of constitutional democracy: that extraordinary powers are exceptional

---

[13] Porcedda M.-G. On the Compatibility of Pandemic Data-Driven Measures with the Right to Data Protection: A Review of 'Under-the-Radar' Measures Adopted in Ireland to Contain COVID-19. Northern Ireland Legal Quarterly, Vol. 73, No. 2, 2022, pp. 310–340. https://doi.org/10.53386/nilq.v73i2.962

[14] European Convention on Human Rights. Signed in Rome on 4 November 1950 [in the wording of 1 June 2010].

[15] CJEU judgment of 6 October 2020 in joined cases No. C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others.

by design and must not evolve into a permanent mode of governance.[16] This temporal element is crucial for data protection: data-collection and surveillance measures must expire once the emergency ends, with deletion of personal data and restoration of full legal safeguards.[17]

The temporary character of emergency measures also implies their reversibility – that is, the restoration of ordinary legal order, institutional checks, and full enjoyment of fundamental rights. As such, temporality operates as both a procedural safeguard and a substantive constitutional guarantee against the normalisation of extraordinary powers.

2. Extraordinary situations and data protection risks

Extraordinary situations amplify the tension between efficiency and human rights. Such situations impose urgency, largescale impact, and often require rapid deployment of technical or organisational solutions. Member States across the EU – during the COVID-19 pandemic for example – introduced contact-tracing apps, location-based mobility tracking systems and large scale data-sharing arrangements (including between public bodies and telecom operators) to stem contagion. However, the European Parliament's briefing on the impact of COVID-19 measures noted that many Member States resorted to emergency powers and "digital and big-data processing measures" with potential implications for privacy and data protection.[18]

These Member States' responses, whilst understandable from a public-health or security perspective, pose serious risks for personal data protection: mass collection of data, surveillance by design, bypassing of prior impact assessment, lack of public consultation, and insufficient exit or "sunset" clauses. Scientific analyses emphasise that data processing measures deployed under crisis conditions frequently conflict with the general principles of data protection[19] – such as purpose limitation, data-minimisation, transparency and accountability – all of which are core to the General Data Protection Regulation (GDPR)[20] and the Charter.

---

[16] Ackerman B. A. 2004, p. 1045.

[17] European Data Protection Board. Statement on the data protection impact of the interoperability of contact tracing apps of 16 June 2020, pp. 4–5. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf [last viewed 03.11.2025].

[18] European Parliament. The Impact of Covid-19 Measures on Democracy, the Rule of Law and Fundamental Rights in the EU, pp. 1–2. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651343/IPOL_BRI(2020)651343_EN.pdf [last viewed 03.11.2025].

[19] Newlands G., Lutz C., Tamo-Larrieux A., Fosch Villaronga E., Harasgama R., Scheitlin G. Innovation under Pressure: Implications for Data Privacy During the Covid-19 Pandemic. Big Data & Society, Vol. 7, No. 2, 2020, pp. 6–8. https://doi.org/10.1177/2053951720976680

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [last viewed 03.11.2025].

For example, in the Irish context Porcedda's study shows that "under-the-radar" data-driven measures (thermal scanner guns, self-check forms, vaccine information systems) partly failed to comply with the right to data protection because they lacked systematic strategy, transparency, or sunset provisions.[21] Newlands et al. noted that rushed implementation leads to function creep: data initially collected for public-health purposes may later serve law-enforcement.[22] Such developments erode the principle of purpose limitation enshrined in Article 5(1)(b) GDPR.

In addition, the judicial review of COVID-19 related measures in EU Member States provides a valuable empirical basis for analysing how constitutional courts and supreme jurisdictions have balanced emergency powers against fundamental rights, particularly the rights to privacy and personal data protection. The COVID-19 Litigation Database[23] (an open-access repository of case law developed by the University of Trento and the World Health Organisation) offers an extensive collection of such judgments across Europe. According to this database, 25 decisions from various EU Member States' constitutional and supreme courts address privacy and data-protection issues arising during the pandemic. It should be noted, however, that this figure is not exhaustive, as not all Member States are equally represented and certain national decisions remain unpublished or unreported. A quantitative overview of these decisions reveals that in 10 out of 25 cases (approximately 40%), the courts concluded that governmental measures adopted under the state of emergency unlawfully restricted the fundamental rights to privacy or personal data protection.

This finding indicates a significant risk that extraordinary situations and the exercise of extraordinary powers – particularly when implemented through digital surveillance, health data collection, or mobility tracking – may undermine constitutional guarantees of data protection and private life. It also highlights a broader tension within European constitutionalism: although emergency measures are intended to protect public safety and security, they frequently test the resilience of the rule of law and the application of the proportionality principle in safeguarding individual rights. Accordingly, this underscores the need to develop a Governance Framework for Safeguarding Data Protection in Extraordinary Situations.

3. Legal framework: Fundamental rights, GDPR and proportionality

Under EU law, the right to data protection is a qualified right: it may be limited but only subject to the conditions set out in Article 52(1) of the Charter – limits must be: (a) provided by law, (b) pursue a legitimate aim, (c) be necessary

[21] Porcedda M.-G. 2022, pp. 333–334.

[22] Newlands G. et al. 2020, p. 2.

[23] Available: https://www.covid19litigation.org/case-index [last viewed 03.11.2025].

and proportionate, and (d) respect the essence of the right. As European Data Protection Board noted in various documents relating to COVID-19 pandemic measures, even during emergencies the essence of the right under Article 8 of the Charter must be preserved.[24] Such approach was further elaborated in EUCJ jurisprudence, e.g. in La Quadrature du Net case.

In such context, as relates to personal data protection essence, the GDPR provides specific mechanisms – including general principles for processing of personal data (Art. 5), requirements for lawfulness of personal data processing (Art. 6 and 9), obligation to perform data protection impact assessment (DPIA) (Art. 35). The need for DPIAs is highlighted in various documents, such as European Data Protection Board guidelines 04/2020.[25] Thus, the legal framework in extraordinary situations must reconcile three dimensions: (i) the urgent public interest; (ii) the fundamental right to data protection; and (iii) state accountability and oversight.

4. Emerging standards

Case law from EU Member States, data protection supervisory authorities and academic commentary illustrate emerging standards. For instance, the European Data Protection Board in its guidance on location-data and tracing apps stressed that restrictions on rights must (i) be based on law, (ii) pursue a legitimate aim, (iii) be necessary and proportionate, and (iv) include safeguards and a sunset clause.[26] The European Commission's communication on apps supporting the fight against COVID 19 pandemic emphasised interoperability, data-minimisation, voluntary participation and limited retention.[27]

---

[24] For example, European Data Protection Board & European Data Protection Supervisor. Joint Opinion 1/2022 on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/953 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic of 14 March 2022. Available: https://www.edpb.europa.eu/system/files/2022-03/edpb-edps_1-2022_joint_opinion_extension_of_covid_certification_regulation_en.pdf [last viewed 03.11.2025].

[25] European Data Protection Board. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak of 21 April 2020. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf [last viewed 03.11.2025].

[26] European Data Protection Board. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak of 21 April 2020. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf [last viewed 03.11.2025].

[27] Communication from the European Commission. Guidance on Apps Supporting the Fight against COVID-19 Pandemic in Relation to Data Protection (2020/C 124 I/01). Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0417(08)#ntr1-CI2020124EN.01000101-E0001 [last viewed 03.11.2025].

From these and other analyses[28] the following emerging standards can be derived for data-processing in extraordinary situations: (a) lawfulness and legal basis (extraordinary measures must be grounded in law and clearly defined; application of *lawfulness, fairness and transparency* principle); (b) legitimate aim (the emergency measure addresses a genuine extraordinary situation objective, e.g., epidemic control, migrant and refugee control, etc.; application of *purpose limitation* principle); (c) necessity and proportionality (the data-processing must be strictly limited to what is required; application of *data minimization* principle); (d) time-limitation / sunset clause (extraordinary data-processing measures should expire once the official extraordinary situation ends; application of *storage limitation* principle; (e) transparency and accountability (affected individuals should have information and rights of redress); (f) safeguards for vulnerable groups (additional protections for disadvantaged or marginalised populations); and (g) independent review and oversight (judicial or administrative review mechanisms must be accessible).

5. Governance framework for safeguarding data protection in extraordinary situations

Drawing on judicial reasoning and academic analysis, a constitutional-compliance framework can be developed to ensure that emergency measures involving data processing remain lawful, proportionate, and temporary. The framework may be structured around three principal phases: declaration, application, and termination and restoration.

5.1. Declaration phase

At the outset, it is essential to verify the legal and factual grounds for declaring an official extraordinary situation and to ensure that the nature and scope of the threat are clearly defined. Only constitutionally authorised bodies should be empowered to proclaim such an extraordinary situation, consistent with the principle of legality and separation of powers. Even under conditions that restrict regular parliamentary activity, mechanisms of legislative oversight must remain operational to guarantee democratic accountability.

5.2. Application phase

During the implementation of extraordinary measures, it must be ensured that only duly empowered entities exercise extraordinary powers and that these powers are applied strictly within their constitutional and statutory limits. The principle of proportionality requires that all measures affecting personal

[28] For example, Porcedda M.-G. 2022, pp. 310–340.

data be preceded, where feasible, by a rapid DPIA and a human-rights impact assessment. In addition, the deployment of technical and organisational safeguards – such as pseudonymisation, encryption, restricted data access, and real-time auditing mechanisms – is indispensable to minimise intrusiveness and ensure accountability.

5.3. Termination and restoration phase

The temporality of extraordinary regime must be guaranteed through the inclusion of explicit time limits and sunset clauses, after which the extraordinary measures automatically cease to apply. Upon termination of the official extraordinary situation, authorities must ensure the full restoration of ordinary data-protection guarantees, including the erasure or anonymisation of data collected exclusively for extraordinary purposes. This phase symbolises the return to constitutional normality and reaffirms that extraordinary powers are exceptional by design and non-permanent in nature.

Conclusions

1. Extraordinary situations represent a critical stress test for constitutional democracies and their commitment to fundamental rights. This research demonstrates that the right to personal data protection, as enshrined in Article 8 of the Charter, remains fully applicable even under conditions of emergency. While EU law allows for limitations on this right, such limitations must strictly comply with the principles of legality, necessity, proportionality, and respect for the essence of the right.
2. The analysis of constitutional and administrative case law from EU Member States reveals that emergency data processing measures are particularly vulnerable to disproportionality. Courts have repeatedly identified deficiencies related to insufficient legal bases, overly broad data collection, lack of time limits, and inadequate safeguards. These findings confirm that extraordinary circumstances do not justify the suspension of constitutional standards, but rather require their careful and context-sensitive application.
3. On the basis of judicial practice and academic analysis, this research proposes a governance framework structured around the phases of declaration, application, and termination of extraordinary measures. Such a framework emphasises the importance of *ex ante* assessment, ongoing oversight, and effective restoration of ordinary legal order once the crisis subsides. By embedding data protection considerations into each phase of emergency governance, Member States can ensure that crisis responses remain both effective and constitutionally compliant.
4. Ultimately, safeguarding personal data protection during extraordinary situations is not an obstacle to effective governance but a prerequisite for

maintaining public trust, democratic legitimacy, and the rule of law in times of crisis.

BIBLIOGRAPHY

Literature

1. Ackerman B. The Emergency Constitution. Yale Law Journal, Vol. 113, No. 5, 2004, pp. 1029–1092. https://doi.org/10.2307/4135710
2. Bellenghi G. The European Parliament's Proposal for an EU State of Emergency Clause: A Comparative and Constitutional Analysis. Croatian Yearbook of European Law & Policy, Vol. 20, No. 1, 2024, pp. 1–30. https://doi.org/10.3935/cyelp.20.2024.586
3. European Union Agency for Fundamental Rights. Handbook on European Data Protection Law – 2018 edition. Vienna: European Union Agency for Fundamental Rights (FRA), 2018.
4. Lintott A. The Constitution of the Roman Republic. Oxford: Oxford University Press, 1999 (reprinted 2009).
5. Newlands G., Lutz C., Tamo-Larrieux A., Fosch Villaronga E., Harasgama R., Scheitlin G. Innovation under Pressure: Implications for Data Privacy During the Covid-19 Pandemic. Big Data & Society, Vol. 7, No. 2, 2020, pp. 1–14. https://doi.org/10.1177/2053951720976680
6. Porcedda M.-G. On the Compatibility of Pandemic Data-Driven Measures with the Right to Data Protection: A Review of 'Under-the-Radar' Measures Adopted in Ireland to Contain COVID-19. Northern Ireland Legal Quarterly, Vol. 73, No. 2, 2022, pp. 310–340. https://doi.org/10.53386/nilq.v73i2.962

Court practice

7. CJEU judgment of 6 October 2020 in joined cases No. C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others.

Other materials

8. Basic Law for the Federal Republic of Germany. Available: https://www.gesetze-im-internet.de/englisch_gg/ [last viewed 03.11.2025].
9. Charter of Fundamental Rights of the European Union. Proclaimed in Nice on 07.12.2000 [in the wording of 01.12.2009].
10. Communication from the European Commission. Guidance on Apps Supporting the Fight against COVID-19 Pandemic in Relation to Data Protection (2020/C 124 I/01). Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0417(08)#ntr1-CI2020124EN.01000101-E0001 [last viewed 03.11.2025].
11. Constitution of the Republic of Latvia. Available: https://saeima.lv/en/about-saeima/work-of-the-saeima/constitution/ [last viewed 03.11.2025].
12. Constitution of the Republic of Lithuania. Available: https://www.lrs.lt/home/Konstitucija/Constitution.htm [last viewed 03.11.2025].
13. COVID-19 Litigation Database. Available: https://www.covid19litigation.org/case-index [last viewed 03.11.2025].

14. European Convention on Human Rights. Signed in Rome on 4 November 1950 [in the wording of 1 June 2010].
15. European Data Protection Board. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak of 21 April 2020. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf [last viewed 03.11.2025].
16. European Data Protection Board. Statement on the data protection impact of the interoperability of contact tracing apps of 16 June 2020. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statementinteroperability-contacttracingapps_en_0.pdf [last viewed 03.11.2025].
17. European Data Protection Board & European Data Protection Supervisor. Joint Opinion 1/2022 on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/953 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic of 14 March 2022. Available: https://www.edpb.europa.eu/system/files/2022-03/edpb-edps_1-2022_joint_opinion_extension_of_covid_certification_regulation_en.pdf [last viewed 03.11.2025].
18. European Parliament. The Impact of Covid-19 Measures on Democracy, the Rule of Law and Fundamental Rights in the EU. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651343/IPOL_BRI(2020)651343_EN.pdf [last viewed 03.11.2025].
19. European Parliamentary Research Service. States of Emergency in Response to the Coronavirus Crisis: Normative Response and Parliamentary Oversight in EU Member States during the First Wave of the Pandemic, EPRS Study PE 659.385. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/659385/EPRS_STU(2020)659385_EN.pdf [last viewed 03.11.2025].
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [last viewed 03.11.2025].
21. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. Signed in Lisbon on 13 December 2007 [in the wording of 1 December 2009].