SUMMARY OF

ELECTION OBLIGATIONS AND STANDARDS FOR DATA PRIVACY

THE
CARTER CENTER

The Carter Center was founded in 1982 by former U.S. President Jimmy Carter and his wife, Rosalynn, in partnership with Emory University, to advance peace and health worldwide. A not-for-profit, nongovernmental organization, the Center has helped to improve life for people in 90 countries by resolving conflicts; advancing democracy, human rights, and economic opportunity; preventing diseases; and improving mental health care. Please visit www.cartercenter.org to learn more about The Carter Center.

SUMMARY OF

ELECTION OBLIGATIONS AND STANDARDS FOR DATA PRIVACY

THE
CARTER CENTER

One Copenhill
453 John Lewis Freedom Parkway
Atlanta, GA 30307
(404) 420-5100

www.cartercenter.org

Contents

Purpose of This Guide 3

Introduction 7

Summary of Issues and Assessment Criteria 8

 Election Management 8

 Voter Registration 8

 Candidacy and Campaigning 9

 The Media 9

 Voting Operations 9

 Vote Counting and Tabulation 10

 Electoral Dispute Resolution 10

References 11

Purpose of This Guide

This document is a short summary supplement to the Carter Center's Election Obligations and Standards (EOS) handbook and database (https://eos.cartercenter.org). The EOS handbook provides detailed documentation regarding relevant international obligations, standards, and best practices for 10 main parts of the electoral process.

This supplemental EOS series aims to provide a more targeted view of obligations, standards, and best practices related to several specific topics. In this volume, you will find relevant obligations and standards for elections related to data privacy, divided by each part of the election process cycle, followed by endnotes with international documentation and references. (Only the categories with relevant key issues to data privacy are included.)

The key issues and related obligations are presented in black text, followed by the relevant assessment criteria with text color based on the level of the source:

Green is used for international and regional treaties.

Blue is used for political commitments, such as declarations and other commitments that indicate state practice or customary law.

Gold is used for interpretive documents, such as the interpretation of treaty obligations by international courts or treaty monitoring mechanisms.

Background on Election Obligations and Standards

Public international law is the system of laws governing interactions between states. As such, it creates a framework of commonly recognized norms and standards for democratic elections that states have accepted and voluntarily obligated themselves to, through their signature and ratification of treaties, and through their membership in the community of states. The Carter Center's EOS documents use a public international framework to provide a comprehensive tool to assist in reviewing and assessing key election issues.

The EOS framework can be envisioned as a two-dimensional system, with 21 fundamental rights, obligations, and standards on one side (see Chart 1) and 10 categories or "parts" of the electoral cycle on the other (see Chart 2). Using this system, the EOS database categorizes key content derived from roughly 300 source documents of public international law, along with more than 400 assessment criteria, to aid analysts in their work. Chart 3 illustrates the intersection of the 21 main election obligations with the 10 main parts of the electoral process cycle.

Chart 1: Obligations for Democratic Elections

Chart 2: Parts of the Electoral Process

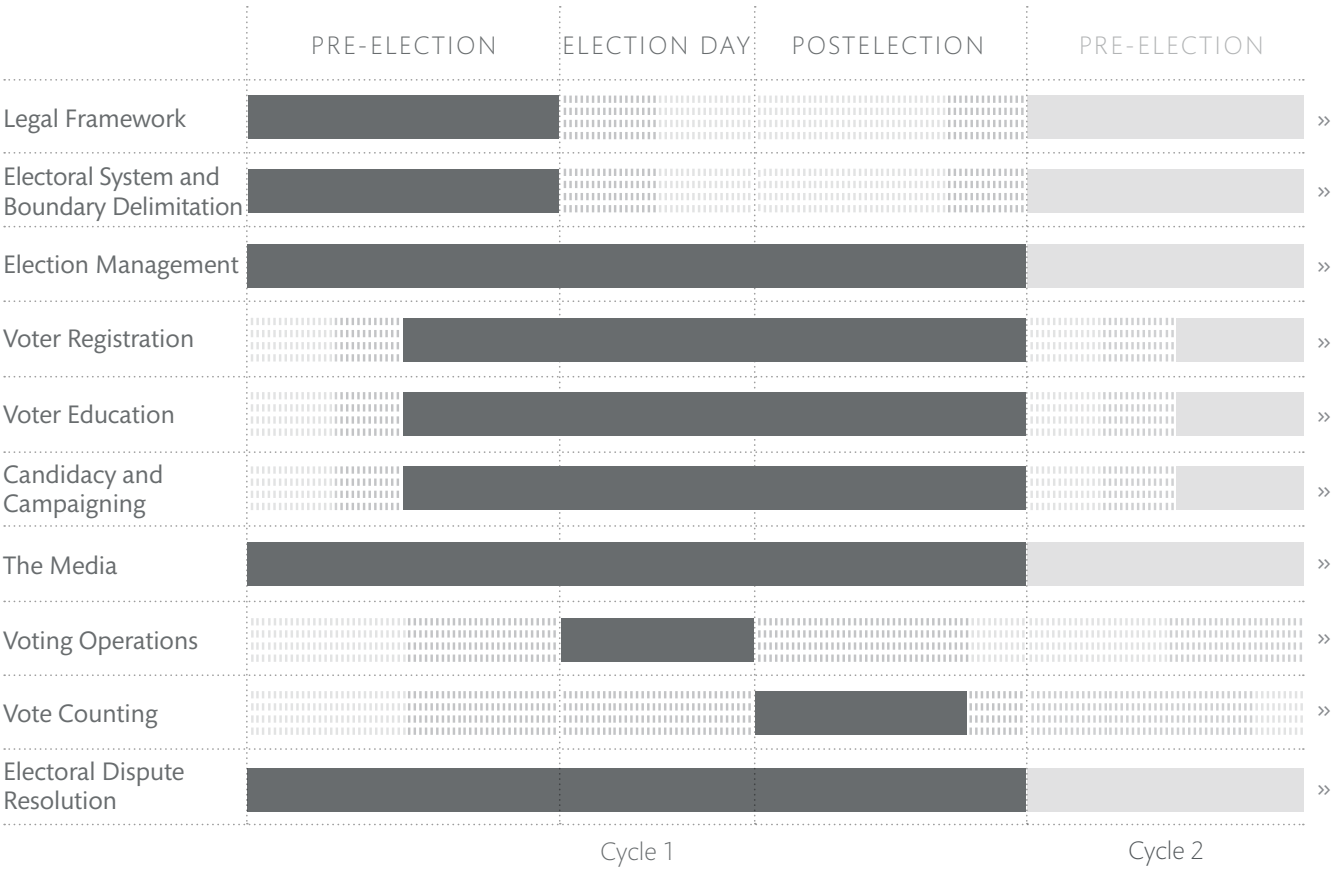

Chart 3: Relevant Obligations

	LEGAL FRAMEWORK	ELECTORAL SYSTEM AND BOUNDARY DELIMITATION	ELECTION MANAGEMENT	VOTER REGISTRATION	VOTER EDUCATION	CANDIDACY AND CAMPAIGNING	THE MEDIA	VOTING OPERATIONS	VOTE COUNTING AND TABULATION	ELECTORAL DISPUTE RESOLUTION
Genuine Elections That Reflect the Free Expression of the Will of the People	●	●	●	●	●	●	●	●	●	●
Right and Opportunity to Vote	●			●	●			●	●	
Right and Opportunity to Be Elected						●		●		
Right and Opportunity to Participate in Public Affairs	●	●	●	●	●	●		●	●	
Freedom of Association	●			●	●	●		●	●	
Freedom of Assembly	●					●				
Freedom of Movement			●	●		●	●	●	●	
Freedom of Opinion and Expression						●	●			
Transparency and Access to Information	●		●	●		●	●	●	●	●
Right to Security of the Person	●		●	●		●	●	●	●	●
Freedom From Discrimination and Equality Before the Law	●	●	●	●	●	●	●	●	●	●
Equality Between Men and Women	●	●	●	●	●	●	●	●	●	●
Right to a Fair and Public Hearing			●							●
Right to an Effective Remedy	●	●	●	●	●	●	●	●	●	●
Universal Suffrage				●	●			●	●	
Equal Suffrage		●		●	●			●	●	
Secret Ballot					●			●	●	
Periodic Elections	●	●	●	●	●	●		●	●	●
Prevention of Corruption	●		●	●		●	●	●	●	●
State Must Take Necessary Steps to Give Effect to Rights	●	●	●	●	●	●	●	●	●	●
Rule of Law	●	●	●	●	●	●	●	●	●	●

● Macro-Level Obligation
● Individual Rights and Freedoms
● Process-Focused Obligations
● Foundational Obligations

Introduction*

Personal data is essential to the conduct of genuine democratic elections. The key parts of election processes such as voter registration, voter education, political campaigning, voter authentication, voting, and vote transmission involve collecting, verifying, or using sensitive personal data of individuals. The types of data obtained or used by election actors have expanded over the years as technology has advanced and can range from physical addresses, medical records, and demographic information to biometric data and facial imaging. The application of digitalized storage and processing systems in elections also has been accompanied by increased capacities of election administrators and others to collect, store, and analyze data, with emerging actors (internet intermediaries, social media platforms, technology vendors, and data analytics companies) playing an increasing role.

While the use of personal data can help prevent fraud and ensure credibility in election processes, improperly managed or misused data can undermine individual privacy, universal suffrage, and genuine electoral competition. Thus, the authority of states to seek, receive, and grant access to data about a person is bound by the obligation to protect individual rights to privacy. Effective data privacy measures, which help guarantee that individuals retain control over the use of their personal data throughout the election cycle, should be anchored on principles of transparency, confidentiality, relevance, accuracy, and accountability.[1]

The right to privacy is well articulated in public international law and was first proclaimed in Article 21 of the Universal Declaration of Human Rights in 1948. It has subsequently been enshrined in several key international and regional human rights instruments, including Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 8 of the European Convention on Human Rights, Article 11 of the American Convention on Human Rights, and Article 21 of the ASEAN Human Rights Declaration. The U.N. Human Rights Committee, mandated to monitor the implementation of the ICCPR, clarified in its General Comment 16 (Paragraph 10) that the right to privacy requires states to take effective measures to ensure that personal data or information about a person's private life is not accessed by public entities (election management bodies) or private entities (business enterprises) that are not authorized by law to receive or access it. In recent years, a growing number of instruments have specified practical measures and standards for states to protect data privacy. These include the African Union Convention on Cyber Security and Personal Data, the Council of Europe Convention 108+, the European Union's General Data Protection Regulation, the Asia-Pacific Economic Cooperation Privacy Framework, the Organization of American States Model Law on Protection of Personal Data, and the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy.

The principles and norms embedded in these instruments apply to elections administration. Collectively, they call on states to implement legal mechanisms, with procedures for data collection and management, to fulfill their data privacy obligations. In other words, the way state authorities and private entities acquire and process personal data should be governed by law. The normative standard for effective data protection also includes the need for clear and transparent data collection and processing based on the informed consent or knowledge of the person whose data is being processed. This extends to the need for data controllers to provide accessible policies about their data processing procedures. It is also clear that personal information should be relevant, implying that data collection, processing, and distribution should be minimal, necessary, and limited to a specified legitimate purpose. Moreover, norms around accuracy stress the need for data controllers to collect and store accurate information, with clear procedures for individuals to request that inaccurate data be corrected or eliminated. Principles of confidentiality and accountability call on states to take data security measures to protect the private nature of personal data, including preventing unauthorized access or loss, and that those who handle or process personal data should operate within mechanisms that ensure compliance with procedures for protecting data privacy.

*This introduction was written by Obehi Okojie, Ph.D., a senior program associate at The Carter Center who specializes in democratic election standards and citizen political participation. He holds a doctorate in juridical science.

Election Management

State Authorities Responsible for Upholding Rights – Access to Information

- An independent, duly resourced body oversaw compliance with data protection principles.[2]

Protection of Personal Data – Access to Information

- Citizens that offered proof of identity had the right to rectify information about them that was inaccurate.[3]
- Personal data collected was not used for other purposes.[4]
- Personal data could be collected and processed based on informed consent.[5]
- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[6]
- An independent, duly resourced body oversaw compliance with data protection principles.[7]
- Everyone had the right to know whether information about themselves was processed and to obtain such information in an accessible format.[8]
- Personal data controllers provided clear and accessible information about their data collection and processing policies and practices.[9]

Voter Registration

Correction of Voter Registration Data – Right to Remedy and Necessary Steps to Rights

- Citizens that offered proof of identity had the right to rectify information about them that was inaccurate.[10]
- Voter registration procedures allowed for claims (of unjustified exclusion) and objections (for incorrect inclusion).[11]

Privacy and Voter Registration – Access to Information and Freedom From Discrimination

- Personal data collected was not used for other purposes.[12]
- The voter list did not include information beyond that necessary to identify a voter and establish his or her eligibility.[13]
- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[14]

Protection of Personal Data – Access to Information

- Citizens that offered proof of identity had the right to rectify information about them that was inaccurate.[15]
- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[16]
- Everyone had the right to know whether information about themselves was processed and to obtain it in an accessible format.[17]
- Personal data controllers provided clear and accessible information about their data collection and processing policies and practices.[18]

Key: **Green** = International and regional treaties; **Blue** = Political commitments; **Gold** = Interpretive documents

Candidacy and Campaigning

Internet and Exercise of Rights Online – Freedom of Assembly

- Internet freedom and the exercise of human rights online were protected. Restrictions imposed were based in law, proportionate, and necessary in a democratic society.[19]

Protection of Personal Data – Access to Information

- Personal data collected was not used for other purposes.[20]
- Personal data could be collected and processed based on informed consent.[21]
- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[22]

The Media

Internet and Exercise of Rights Online – Freedom of Assembly

Internet freedom and the exercise of human rights online were protected. Restrictions imposed were based in law, proportionate, and necessary in a democratic society.[23]

Internet intermediaries were transparent and provided easy access to their policies and practice on online content management, distribution, and automated processing.[24]

Protection of Personal Data – Access to Information

Personal data could be collected and processed based on informed consent.[25]

Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[26]

Personal data controllers provided clear and accessible information about their data collection and processing policies and practices.[27]

Internet intermediaries were transparent and provided easy access to their policies and practice on online content management, distribution, and automated processing.[28]

Business and Protection of Human Rights – Access to Information and Freedom From Discrimination

Personal data controllers provided clear and accessible information about their data collection and processing policies and practices.[29]

Internet intermediaries were transparent and provided easy access to their policies and practice on online content management, distribution, and automated processing.[30]

Business enterprises embraced, in policy and practice, their international and/or national human rights obligations. Accessible and effective complaint and redress mechanisms were established to protect these rights.[31]

Voting Operations

Protection of Personal Data – Transparency and Access to Information

- Personal data collected was not used for other purposes.[32]
- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[33]

Key: **Green** = International and regional treaties; **Blue** = Political commitments; **Gold** = Interpretive documents

Vote Counting and Tabulation

Protection of Personal Data – Access to Information

- Personal data controllers complied with data minimization, accuracy, confidentiality, integrity, and storage limitation obligations.[34]

Electoral Dispute Resolution

Business and Protection of Human Rights – Right to Remedy

- Business enterprises embraced, in policy and practice, their international and/or national human rights obligations. Accessible and effective complaint and redress mechanisms were established to protect these rights.[35]

Key: **Green** = International and regional treaties; **Blue** = Political commitments; **Gold** = Interpretive documents

References

1 Privacy International, A Gude for Policy Engagement on Data Protection: Part 3 Data Collection Principles, posted Aug.30, 2018

2 EU, GDPR, art. 51.1

3 EU, GDPR, art. 5(1)d; U.N. (CCPR), General Comment 34, para. 18; U.N. (CCPR), General Comment 16, para. 10

4 EU, GDPR, art. 5(1)b; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7.c; CoE (Committee of Ministers), Recommendation (2012)4 on the Protection of Human Rights with Regard to Social Networking Services, para. 6; CoE (Committee of Ministers), Recommendation on Good Administration, art. 9.1-3; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

5 EU, GDPR, art. 6.1.a; CoE (Committee of Ministers), Recommendation (2018)2, para. 2.4.2; APEC, Privacy Framework, para. 25

6 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8; EU, GDPR, art. 5.1.e; EU, GDPR, art. 5.1.d, f

7 EU, GDPR, art. 51.1

8 U.N., ICCPR, art. 19(2); AU, AfCHPR, art. 9(1); OAS, ACHR, art. 13(1); LAS, Arab Charter, art. 32; CoE, ECHR, art. 10(1); CIS, Convention on Human Rights, art. 11(1); EU, GDPR, art. 5(1)d; U.N. (CCPR), General Comment 34, para, 18; U.N. (CCPR), General Comment 16, para. 10

9 EU, GDPR, art. 5(1)a; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 12; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7(b); CoE (Committee of Ministers), Recommendation (2018)2 on the Roles and Responsibilities of Internet Intermediaries, para. 2.2.1–3

10 EU, GDPR, art. 5(1)d; U.N. (CCPR), General Comment 34, para. 18; U.N. (CCPR), General Comment 16, para. 10

11 EU, Handbook (Ed. 2), p. 44

12 EU, GDPR, art. 5(1)b; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7.c; CoE (Committee of Ministers), Recommendation (2012)4 on the Protection of Human Rights with Regard to Social Networking Services, para. 6; CoE (Committee of Ministers), Recommendation on Good Administration, art. 9.1–3; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8 ; CoE, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. art. 5; EU, GDPR, art. 5(1)b; APEC, Privacy Framework, para. 25; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8 ; U.N., ICCPR, art. 17

13 UNGA, Guidelines Concerning Computerized Data Files, art. 3

14 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3 on the Protection of Human Rights with Regard to Search Engines, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

15 EU, GDPR, art. 5(1)d; U.N. (CCPR), General Comment 34, para. 18; U.N. (CCPR), General Comment 16, para. 10

16 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3 on the Protection of Human Rights with Regard to Search Engines, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

17 U.N., ICCPR, art. 19(2); AU, AfCHPR, art. 9(1); OAS, ACHR, art. 13(1); LAS, Arab Charter, art. 32; CoE, ECHR, art. 10(1); CIS, Convention on Human Rights, art. 11(1) ; EU, GDPR, art. 5(1)d; U.N. (CCPR), General Comment 34, para, 18; U.N. (CCPR), General Comment 16, para. 10

18 EU, GDPR, art. 5(1)a; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 12; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7(b); CoE (Committee of Ministers), Recommendation (2018)2 on the Roles and Responsibilities of Internet Intermediaries, para. 2.2.1–3

19 CoE (Committee of Ministers), Declaration CM(2005)56, para. I.1; CoE (Committee of Ministers): Recommendation (2016)5, para. 2(4)1; UNHRC, Resolution 38/7, para. 1; U.N. (CCPR), General Comment No. 37, para. 34; CoE (PACE), Resolution 2256(2019), para. 3; CoE (Committee of Ministers), Recommendation (2016)5, para. 2-3; IPU, Declaration on Criteria for Free and Fair Elections, art. 4(3)

20 EU, GDPR, art. 5(1)b; UNGA, Resolution 73/179, para. 7.c; CoE (Committee of Ministers), Recommendation (2012)4, para. 6; CoE (Committee of Ministers), Recommendation on Good Administration, art. 9.1-3; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

21 EU, GDPR, art. 6.1.a; CoE (Committee of Ministers), Recommendation (2018)2, para. 2.4.2; APEC, Privacy Framework, para. 25

22 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

23 CoE (Committee of Ministers), Declaration CM(2005)56, para. I.1; CoE (Committee of Ministers): Recommendation (2016)5, para. 2(4)1; UNHRC, Resolution 38/7, para. 1; U.N. (CCPR), General Comment No. 37, para. 34; CoE (PACE), Resolution 2256(2019), para. 3; CoE (Committee of Ministers), Recommendation (2016)5, para. 2–3

24 U.N. (OHCHR), Guiding Principles on Business and Human Rights, para. II.A.11-13; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, Recommendation (2016)1, para. 5.1, Recommendation (2018)2, para. 2.2.3; EU (European Commission), Recommendation on Measures to Effectively Tackle Illegal Content Online, para. 16

25 EU, GDPR, art. 5(1)b; UNGA, Resolution 73/179, para. 7.c; CoE (Committee of Ministers), Recommendation (2012)4, para. 6; CoE (Committee of Ministers), Recommendation on Good Administration, art. 9.1–3; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8; EU, GDPR, art. 6.1.a; CoE (Committee of Ministers), Recommendation (2018)2, para. 2.4.2;

APEC, Privacy Framework, para. 25

26 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8; EU, GDPR, art. 5.1.e; EU, GDPR, art. 5.1.d, f; CoE (Committee of Ministers), Recommendation (2018)2, para. 2.5.1-3, Recommendation (2016)1, para. 6.1; U.N. (OHCHR), Freedom of Expression and Elections in the Digital Age, p. 13

27 EU, GDPR, art. 5(1)a; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 12; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7(b); CoE (Committee of Ministers), Recommendation (2018)2 on the Roles and Responsibilities of Internet Intermediaries, para. 2.2.1-3

28 U.N. (OHCHR), Guiding Principles on Business and Human Rights, para. II.A.11-13; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, Recommendation (2016)1, para. 5.1, Recommendation (2018)2, para. 2.2.3; EU (European Commission), Recommendation on Measures to Effectively Tackle Illegal Content Online, para. 16

29 EU, GDPR, art. 5(1)a; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 12; UNGA, Resolution 73/179 on the Right to Privacy in the Digital Age, para. 7(b); CoE (Committee of Ministers), Recommendation (2018)2 on the Roles and Responsibilities of Internet Intermediaries, para. 2.2.1-3

30 U.N. (OHCHR), Guiding Principles on Business and Human Rights, para. II.A.11-13 ; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, Recommendation (2016)1, para. 5.1, Recommendation (2018)2, para. 2.2.3; EU (European Commission), Recommendation on Measures to Effectively Tackle Illegal Content Online, para. 16

31 CoE (Committee of Ministers), Recommendation (2012)3, para. 7, Recommendation (2016)1, para. 5.1, Recommendation (2018)2, para. 2.2.3; EU (European Commission), Recommendation on Measures to Effectively Tackle Illegal Content Online, para. 16

32 EU, GDPR, art. 5(1)b; UNGA, Resolution 73/179, para. 7.c; CoE (Committee of Ministers), Recommendation (2012)4, para. 6; CoE (Committee of Ministers), Recommendation on Good Administration, art. 9.1–3; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

33 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8; EU, GDPR, art. 5.1.e

34 EU, GDPR, art. 5(1)b,c; CoE (Committee of Ministers), Recommendation (2012)3, para. 7, 10; APEC, Privacy Framework, para. 24; OECD, Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, para. 8

35 CoE (Committee of Ministers), Recommendation (2018)2, para. 2.5.1-3, Recommendation (2016)1, para. 6.1; U.N. (OHCHR), Freedom of Expression and Elections in the Digital Age, p. 13

THE
CARTER CENTER

One Copenhill
453 John Lewis Freedom Parkway
Atlanta, GA 30307
(404) 420-5100

www.cartercenter.org