Security Industry Association (SIA)
Privacy Profile References

GDPR References for Physical Security & Identity in the U.S.¹

1 v.1 (please send all comments to security@openconsent.com)
# Table of Contents

**USA**

Privacy Act

European Union (EU)-U.S. Privacy Shield

Federal Information Security Management Act (FISMA)

National Conference of State Legislatures

Children’s Online Privacy Protection Rule (COPPA)


The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records

Gramm-Leach-Bliley Act (GLBA)

Fair Credit Reporting Act (FCRA)

California

- Assembly Bill No. 375 – Privacy: Personal Information: Businesses
- California Consumer Privacy Act (CCPA)

Privacy Journal

U.S. Privacy Laws by State

**Europe**

EU

- The General Data Protection Regulation (GDPR)
- EU Charter of Fundamental Rights
- Council of Europe: The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No. 108)
- The Data Protection Law Enforcement Directive
- ePrivacy Directive
European Court of Justice (ECJ) ....................................................................................................... 8

CASE AT.39740  Google Search (Shopping) ...................................................................................... 8

Judgment in Case C-131/12
Google Spain SL, Google Inc. v Agencia Española de Protección de Datos ................. 8

Incorporation of the GDPR Into the European Economic Area (EEA) Agreement .......... 9

Article 29 Data Protection Working Party .................................................................................... 9

Guidelines on Automated Individual Decision Making
and Profiling for the Purposes of Regulation 2016/679 ....................................................... 9

Guidelines on Transparency Under Regulation 2016/679 ....................................................... 9

Guidelines on Consent Under Regulation 2016/679 ............................................................... 9

International

International Standards Organization (ISO) .................................................................................... 9

ISO 27001 Information Security Management ........................................................................ 9

ISO 27002 Code of Practice for Information Security Controls ........................................ 9

ISO 2900 Privacy Framework ..................................................................................................... 9

ISO 29184 Guidelines for Online Privacy Notices and Consent ........................................... 9

United Kingdom

Data Protection Act (2018) ......................................................................................................... 9

Protection of Freedoms (2012) ................................................................................................. 9

Police and Criminal Evidence Act (1984) ................................................................................. 10

The Privacy and Electronic Communications
(EC Directive) (Amendment) Regulations (2011) ................................................................. 10

UK Information Commissioner’s Office (ICO) ....................................................................... 10

ICO Resources ........................................................................................................................ 10

Guide to 12 Principles ............................................................................................................. 10

Third Party Certification ........................................................................................................ 10
UK Surveillance Commissioner ..........................................................................................................10
Surveillance Camera Code of Practice.............................................................................................10
CCTV Checklist................................................................................................................................10
Surveillance Camera Commissioner’s Buyer’s Toolkit ........................................................................10
UK Sample Risk Assessments and Codes of Practice for CCTV .....................................................10
Nuneaton and Bedworth ....................................................................................................................10
Brent ..................................................................................................................................................10
National Security Inspectorate ........................................................................................................10
Wigan Privacy Impact Assessment ..................................................................................................11
Self-Assessment Tools ......................................................................................................................11
Automatic Number Plate Recognition ..............................................................................................11
Body-Worn Video ..............................................................................................................................11
Safeguarding Body-Worn Video Data ...............................................................................................11
CCTV Assessment Tool ....................................................................................................................11
Unmanned Aerial Vehicles and Drones ............................................................................................11
Data Protection Self-Assessment ...................................................................................................11
Privacy Impact Assessment Template ............................................................................................11
United Kingdom Home Office ..........................................................................................................11
British Standards Institute (BSI) ......................................................................................................11
BSI CCTV Standards (Fees Apply) ..................................................................................................11
British Security Industry Association (BSIA) ....................................................................................12
BSIA Graded Requirements based on BS EN 62676 Standards for CCTV .....................................12
BSIA Maintenance of CCTV Surveillance Systems Code of Practice ...........................................12
BSIA Planning, Design, Installation and Operation of CCTV
Surveillance Systems Code of Practice and Associated Guidance ........................................... 12

### Cloud

- ISO 27018 .......................................................................................................................................... 12
- Protection of Personally Identifiable Information in Cloud ......................................................... 12
- Amazon ISO 27018 Compliance ............................................................................................... 12
- Amazon ISO 27018 Certificate .................................................................................................. 12
  - Information Technology – Cloud Computing – Service-Level Agreement (SLA)
    Framework – Part 3: Core Conformance Requirements ........................................................ 12

### Cloud Security Alliance

- Cloud Controls Matrix .................................................................................................................... 12
- STAR Certification ..................................................................................................................... 12
- Big Data Security and Privacy Handbook ................................................................................ 12
- Certificate of Cloud Security Knowledge ................................................................................. 12

### German Federal Office for Information Security
(Bundesamt fur Sicherheit in der Informationstechnik - BSI) ...................................................... 13

- Secure Use of Cloud Services ................................................................................................... 13

### International Federation of Accountants (IFA)

- International Standard on Assurance Engagements (ISAE) 3402–
  Assurance Reports on Controls at a Service Organization .................................................... 13

- American Institute of Certified Public Accountants (AICPA) ................................................ 13

- Statement on Standards for Attestation Engagements (SAE) #18 ...................................... 13

### Guides

- International Association of Privacy Professionals (IAPP) ...................................................... 13
- GDPR Awareness Guide ............................................................................................................. 13
Privacy Profile References

Microsoft ........................................................................................................................................... 13
GDPR Assessment Guide .............................................................................................................. 13
Axis .................................................................................................................................................... 13
Camera Hardening Guide ........................................................................................................... 13
Milestone Video Management Systems ........................................................................................ 13
Hardening Guide ........................................................................................................................... 13
University of Michigan ..................................................................................................................... 14
Standard Practice Guide – Proper Use of Security Cameras ......................................................... 14
Hikvision (Leading Chinese Manufacturer) .................................................................................... 14
Network Camera Security Guide .................................................................................................. 14

Additional Resources

National Institute of Standards & Technology (NIST) .................................................................... 14
Cybersecurity Framework ............................................................................................................. 14
Digital Identity Guidelines (SP 800-63-3, 800-63A, 800-63B, 800-63C) ........................................... 14
Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev.5 (DRAFT)) ............................................................................................................... 14
Security Industry Association (SIA) ................................................................................................. 14
Open Supervised Device Protocol (OSDP) .................................................................................... 14
International Association of Privacy Professionals (IAPP) ........................................................... 14
Analysis: CCPA (2018) .................................................................................................................... 14
International Electrotechnical Commission (IEC) ........................................................................... 14
Video Surveillance Systems for Use in Security Applications IEC 62676-1-1 Systems Requirements ............................................................................................................................... 14
Cornell University ........................................................................................................................ 14
Responsible Use of Video Surveillance Systems POLICY 8.1 ......................................................... 14
Privacy Profile References

International Data Commissioners ........................................................................................................ 15
Home Page ........................................................................................................................................ 15
Members List ..................................................................................................................................... 15
Privacy Principles .............................................................................................................................. 15
Fair Information Practice Principles (FIPPs) .................................................................................... 15
OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data ........ 15
APEC Privacy Framework (Including Principles) ............................................................................ 15
New Zealand Privacy Commissioner Privacy Principles ................................................................. 15
IDESG Baseline Principles (including Privacy) ................................................................................ 15
Codes of Practice ............................................................................................................................... 15
Australian Security Industry Association Limited ........................................................................ 15
CCTV Code of Ethics ......................................................................................................................... 15
Australian Retailers Association ....................................................................................................... 15
Video Surveillance Code of Practice ................................................................................................. 15
City of Perth ....................................................................................................................................... 15
CCTV Surveillance Operations Code of Practice ............................................................................ 15
Blogs ................................................................................................................................................. 16
Privacy 2.0, Economist ....................................................................................................................... 16
New California Privacy Law to Affect More Than Half a Million U.S. Companies ....................... 16
References

United States

USA

Privacy Act

European Union (EU)-U.S. Privacy Shield

Federal Information Security Management Act (FISMA)
In accordance with FISMA, NIST is responsible for developing standards, guidelines and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems.

National Conference of State Legislatures

Children’s Online Privacy Protection Rule (COPPA)
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule


The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records
https://www.law.cornell.edu/cfr/text/42/part-2

Gramm-Leach-Bliley Act (GLBA)

Fair Credit Reporting Act (FCRA)
California
Assembly Bill No. 375 – Privacy: Personal Information: Businesses
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

California Consumer Privacy Act (CCPA)

Privacy Journal
U.S. Privacy Laws by State
http://www.privacyjournal.net/_center_compilation_of_state_and_federal_privacy_laws__center__3077.htm

Europe

EU
The General Data Protection Regulation (GDPR)

EU Charter of Fundamental Rights

Council of Europe: The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (CETS No. 108)

The Data Protection Law Enforcement Directive
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

ePrivacy Directive

European Court of Justice (ECJ)
CASE AT.39740  Google Search (Shopping)

Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos
Incorporation of the GDPR Into the European Economic Area (EEA) Agreement

Article 29 Data Protection Working Party
Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679

Guidelines on Transparency Under Regulation 2016/679
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Guidelines on Consent Under Regulation 2016/679

International

International Standards Organization (ISO)
ISO 27001 Information Security Management
https://www.iso.org/isoiec-27001-information-security.html

ISO 27002 Code of Practice for Information Security Controls

ISO 2900 Privacy Framework
https://www.iso.org/standard/45123.html

ISO 29184 Guidelines for Online Privacy Notices and Consent
https://www.iso.org/standard/70331.html

United Kingdom

UK
Data Protection Act (2018)

Protection of Freedoms (2012)
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
Police and Criminal Evidence Act (1984)
https://www.legislation.gov.uk/ukpga/1984/60/contents

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011)

**UK Information Commissioner’s Office (ICO)**

ICO Resources
https://ico.org.uk/for-organisations/resources-and-support/

Guide to 12 Principles

Third Party Certification

**UK Surveillance Commissioner**

Surveillance Camera Code of Practice

CCTV Checklist

Surveillance Camera Commissioner’s Buyer’s Toolkit

**UK Sample Risk Assessments and Codes of Practice for CCTV**

Nuneaton and Bedworth

Brent

National Security Inspectorate
Wigan Privacy Impact Assessment

Self-Assessment Tools

Automatic Number Plate Recognition

Body-Worn Video

Safeguarding Body-Worn Video Data

CCTV Assessment Tool

Unmanned Aerial Vehicles and Drones

Data Protection Self-Assessment

Privacy Impact Assessment Template

United Kingdom Home Office


British Standards Institute (BSI)

BSI CCTV Standards (Fees Apply)

British Security Industry Association (BSIA)

BSIA Graded Requirements based on BS EN 62676 Standards for CCTV
https://www.bsia.co.uk/Portals/4/Publications/218-CCTV-graded-requirements-02.pdf


Cloud

ISO 27018
Protection of Personally Identifiable Information in Cloud https://www.iso.org/standard/61498.html


Cloud Security Alliance

Cloud Controls Matrix https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

STAR Certification https://cloudsecurityalliance.org/star/certification/#_overview


Certificate of Cloud Security Knowledge https://cloudsecurityalliance.org/education/ccsk/#_overview
German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI)

Secure Use of Cloud Services

International Federation of Accountants (IFA)

International Standard on Assurance Engagements (ISAE) 3402 – Assurance Reports on Controls at a Service Organization

American Institute of Certified Public Accountants (AICPA)

Statement on Standards for Attestation Engagements (SAE) #18
https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf

Guides

International Association of Privacy Professionals (IAPP)

GDPR Awareness Guide
https://iapp.org/media/pdf/resource_center/GDPR_AWARENESS_GUIDE._092717.pdf

Microsoft

GDPR Assessment Guide
https://assessment.microsoft.com/gdpr-compliance

Axis

Camera Hardening Guide

Milestone Video Management Systems

Hardening Guide
**University of Michigan**

Standard Practice Guide – Proper Use of Security Cameras  
[http://www.spg.umich.edu/policy/606.01](http://www.spg.umich.edu/policy/606.01)

**Hikvision (Leading Chinese Manufacturer)**

Network Camera Security Guide  
[https://www.hikvision.com/ueditor/net/upload/2018-02-28/e8854c0d-0a40-40e8-9c79-2abff-cea2e46.pdf](https://www.hikvision.com/ueditor/net/upload/2018-02-28/e8854c0d-0a40-40e8-9c79-2abff-cea2e46.pdf)

**Additional Resources**

**National Institute of Standards & Technology (NIST)**

Cybersecurity Framework  
[https://www.nist.gov/cyberframework/framework](https://www.nist.gov/cyberframework/framework)

Digital Identity Guidelines (SP 800-63-3, 800-63A, 800-63B, 800-63C)  
[https://pages.nist.gov/800-63-3/](https://pages.nist.gov/800-63-3/)

Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev.5 (DRAFT))  

**Security Industry Association (SIA)**

Open Supervised Device Protocol (OSDP)  

**International Association of Privacy Professionals (IAPP)**

Analysis: CCPA (2018)  

**International Electrotechnical Commission (IEC)**

Video Surveillance Systems for Use in Security Applications IEC 62676-1-1 Systems Requirements  
[https://webstore.iec.ch/publication/7347#additionalinfo](https://webstore.iec.ch/publication/7347#additionalinfo)

**Cornell University**

Responsible Use of Video Surveillance Systems POLICY 8.1; Volume: 8, Risk Management and Public Safety Chapter:1, Issued: April 2, 2009 Last updated: June 12, 2018  
[http://www.dfa.cornell.edu/sites/default/files/policy/vol8_1_0.pdf](http://www.dfa.cornell.edu/sites/default/files/policy/vol8_1_0.pdf)
International Data Commissioners

Home Page
https://icdppc.org/

Members List
https://icdppc.org/participation-in-the-conference/list-of-accredited-members/

Privacy Principles

Fair Information Practice Principles (FIPPs)

OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

APEC Privacy Framework (Including Principles)
https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

New Zealand Privacy Commissioner Privacy Principles

IDESG Baseline Principles (Including Privacy)

Codes of Practice

Australian Security Industry Association Limited
CCTV Code of Ethics

Australian Retailers Association
Video Surveillance Code of Practice

City of Perth
CTV Surveillance Operations Code of Practice
Blogs

Privacy 2.0, Economist
https://www.economist.com/node/15350984/print 2010

New California Privacy Law to Affect More Than Half a Million U.S. Companies
https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/