数据保护条例框架与wik解读

# GDPR

个人数据的控制者和处理者必须*采取适当的技术和组织措施*以实施数据保护原则。在设计和构建处理个人数据的业务流程时，必须考虑到这些原则，并提供保护数据的保护措施（例如，在适当的情况下使用[假名](https://en.wikipedia.org/wiki/Pseudonymization" \o "假名化)或完全[匿名化](https://en.wikipedia.org/wiki/Data_anonymization" \o "数据匿名化)）。数据控制器必须在设计信息系统时考虑到隐私，例如默认情况下使用最高可能的隐私设置，以使数据集默认情况下不公开可用，并且不能用于标识主题。除非根据法规指定的六个合法依据之一进行此处理，否则不得处理个人数据（[同意](https://en.wikipedia.org/wiki/Consent" \o "同意)，合同，公共任务，重大利益，合法利益或法律要求）。当基于同意进行处理时，数据主体有权随时撤消它。

GDPR于2016年4月14日通过，并于2018年5月25日开始生效。由于GDPR是一项[法规](https://en.wikipedia.org/wiki/Regulation_(European_Union)" \o "法规（欧盟）)，而非[指令](https://en.wikipedia.org/wiki/Directive_(European_Union)" \o "指令（欧盟）)，因此具有直接约束力和适用性，但确实为该法规的某些方面提供了灵活性，可以由个人进行调整成员国。

该法规成为欧盟以外许多国家法律的典范：从智利到日本，从巴西到韩国，从阿根廷到肯尼亚。例如，2018年6月28日通过的[《加州消费者隐私法案》](https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act" \o "加州消费者隐私法)（CCPA）与GDPR有很多相似之处。

# 目录[ [编辑](https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&action=edit&section=1" \o "编辑部分：目录)]

GDPR 2016共有11章，涉及一般规定，原则，数据主体的权利，数据控制者或处理者的职责，个人数据向第三国的转移，监管机构，成员国之间的合作，补救措施，因违反规定而承担的责任或处罚权利和其他最终规定。

目录

[第一章 GDPR 1](#_Toc27032)

[第二章 目录[ 编辑] 1](#_Toc21288)

[第三章 1.1I一般规定 2](#_Toc2975)

[第四章 1.2II原则 2](#_Toc5499)

[第五章 1.3III数据主体的权利 2](#_Toc26131)

[第六章 1.4IV控制器和处理器 3](#_Toc20982)

[第1节 1.4.11假名化 3](#_Toc15546)

[第2节 1.4.22加工活动记录（方便事后审查） 3](#_Toc23250)

[第3节 1.4.33个人数据的安全性 3](#_Toc26702)

[第4节 1.4.44数据保护人员 3](#_Toc16319)

[第5节 1.4.5欧盟代表 3](#_Toc21552)

[第七章 1.5VIII救济，责任和处罚 3](#_Toc14144)

[第八章 例外[ 编辑] 3](#_Toc6872)

[第6节 统计和科学分析 4](#_Toc16362)

[第7节 关于劳资关系有专门的法律 4](#_Toc16026)

[第8节 自然人在纯粹的个人或家庭活动过程中处理个人数据 4](#_Toc8327)

[第九章 确定以下国家/地区提供了足够水平的数据保护[](#_Toc10678)*[需要引用](#_Toc10678)*[]： 4](#_Toc10678)

[第十章 Ref 4](#_Toc26226)

[第9节 Do Not Track legislatio不追踪法规 4](#_Toc14292)

[第10节 隐私和电子通讯指令2002 5](#_Toc15265)

[第11节 EU–US Privacy Shield 6](#_Toc23631)

# [1.1I一般规定](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "I_General_provisions)

# [1.2II原则](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "II_Principles)

# [1.3III数据主体的权利](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "III_Rights_of_the_data_subject)

* + [1.3.11透明度和方式](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "1_Transparency_and_modalities)
  + [1.3.22信息和访问](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "2_Information_and_Access)
  + [1.3.33整改](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "3_Rectification_and_erasure)
  + [1.3.44反对权和自动决定权](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "4_Right_to_object_and_automated_decisions)

# [1.4IV控制器和处理器](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "IV_Controller_and_processor)

## [1.4.11假名化](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "1_Pseudonymisation)

GDPR将[假名化](https://en.wikipedia.org/wiki/Pseudonymization" \o "假名化)称为存储数据时所需要的过程（作为对完整[数据匿名化](https://en.wikipedia.org/wiki/Data_anonymisation" \o "数据匿名化)的另一种选择的替代方法）[[23]，](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "cite_note-23)以无法将所得数据归因于特定数据的方式来转换个人数据主题，不使用其他信息。一个例子就是[加密](https://en.wikipedia.org/wiki/Encryption_software" \o "加密软件)，它使原始数据变得难以理解，并且如果不访问正确的[解密密钥，](https://en.wikipedia.org/wiki/Encryption" \o "加密)就无法逆转该过程。GDPR要求将其他信息（例如解密密钥）与假名数据分开保存。

假名化的另一个示例是[令牌化](https://en.wikipedia.org/wiki/Tokenization_(data_security)" \o "令牌化（数据安全性）)，它是一种保护[静止数据](https://en.wikipedia.org/wiki/Data_at_rest" \o "静止数据)的非数学方法，可以用非敏感替代物（称为令牌）替换敏感数据。尽管令牌没有外部或可利用的含义或价值，但它们允许对特定数据完全或部分可见，以便进行处理和分析，同时隐藏敏感信息。令牌化不会改变数据的类型或长度，这意味着可以由可能对数据长度和类型敏感的数据库等传统系统对其进行处理。与传统的加密数据相比，这也需要更少的计算资源来处理，并且数据库中的存储空间也更少。

假名化是一种[增强隐私的技术](https://en.wikipedia.org/wiki/Privacy-enhancing_technologies" \o "增强隐私的技术)，建议使用假名[化](https://en.wikipedia.org/wiki/Privacy-enhancing_technologies" \o "Privacy-enhancing technologies)以降低对相关数据主体的风险，并帮助控制者和处理者履行其数据保护义务（第28条）。[[24]](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "cite_note-24)

## [1.4.22加工活动记录](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "2_Records_of_processing_activities)（方便事后审查）

## [1.4.33个人数据的安全性](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "3_Security_of_personal_data)

## [1.4.44数据保护人员](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "4_Data_protection_officer)

## [1.4.5欧盟代表](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "EU_Representative)

# [1.5VIII救济，责任和处罚](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "VIII_Remedies,_liability_and_penalties)

# 例外[ [编辑](https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&action=edit&section=16" \o "编辑部分：异常)]

|  |  |
| --- | --- |
|  |  |

该法规未涵盖以下情况：[[8]](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \l "cite_note-32016R0679-8) [ *[所需页面](https://en.wikipedia.org/wiki/Wikipedia:Citing_sources" \o "维基百科：引用来源)* ]

* 合法拦截，国家安全，军事，警察，司法

## 统计和科学分析

* 死者须遵守国家法律

## 关于劳资关系有专门的法律

## 自然人在纯粹的个人或家庭活动过程中处理个人数据

# 确定以下国家/地区提供了足够水平的数据保护[ *[需要引用](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "维基百科：需要引用)* ]：

* 安道尔
* 阿根廷
* 加拿大（对于商业实体）
* 法罗群岛
* 根西岛
* 以色列
* 马恩岛
* 日本
* 泽西岛
* 新西兰
* 瑞士
* 乌拉圭
* 美利坚合众国（请参阅“ [隐私盾”](https://en.wikipedia.org/wiki/EU-US_Privacy_Shield" \o "欧美隐私保护盾)）

# Ref

* 欧洲理事会[网络犯罪公约](https://en.wikipedia.org/wiki/Cybercrime_Convention" \o "网络犯罪公约)
* [儿童在线隐私保护法](https://en.wikipedia.org/wiki/Children's_Online_Privacy_Protection_Act" \o "儿童在线隐私保护法)（COPPA）

电子隐私权法规（欧盟）EPrivacy\_Regulation\_(European\_Union)

## Do Not Track legislatio不追踪法规

* 地球图标。
* 本文中的示例和观点主要涉及美国，并不代表对此主题的全球看法。您可以根据需要改进本文，在讨论页面上讨论问题或创建新文章。 （2013年5月）（了解如何以及何时删除此模板消息）
* 不跟踪立法保护了用户选择是否要被第三方网站跟踪的权利。它通常被称为“ 请勿呼叫 ” 的在线版本。[1]该立法得到隐私保护主义者的支持，遭到使用跟踪信息来个性化Web内容的广告商和服务的反对。[ 需要引用 ]参议员霍什·霍利（Josh Hawley）提出了目前正在执行的名为“禁止追踪法”的立法。[2]
* 内容
* 1 概述
* 2 历史
* 3 美国立法
* 3.1 不追踪2019年法案
* 3.2 请勿追踪我的2011年在线法案
* 3.3 加利福尼亚参议院第761号法案
* 3.4 加利福尼亚州议会法案AB 370
* 3.5 1998年《儿童在线隐私保护法》
* 3.6 2011年《消费者隐私保护法》
* 3.7 商业隐私权法案
* 3.8 不追踪2011年在线法案
* 3.9 2011年不追踪儿童法
* 3.10 消费者隐私权利法案
* 3.11 新的商业隐私权利法案
* 3.12 联邦贸易委员会的报告

## 隐私和电子通讯指令2002

**关于隐私和电子通信的隐私和电子通信指令2002/58** / EC，也称为电子隐私**指令**（ePD），是有关数字时代数据保护和隐私的[欧盟指令](https://en.wikipedia.org/wiki/Directive_(European_Union)" \o "指令（欧盟）)。[[1]](https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002" \l "cite_note-:0-1)它代表了早期工作的延续，最直接的是《[数据保护指令》](https://en.wikipedia.org/wiki/Directive_95/46/EC_on_the_protection_of_personal_data" \o "关于个人数据保护的95/46 / EC指令)。它处理许多重要问题的法规，例如信息的保密性，交通数据的处理，[垃圾邮件](https://en.wikipedia.org/wiki/Spam_(electronic)" \o "垃圾邮件（电子）)和[cookie](https://en.wikipedia.org/wiki/HTTP_cookie" \o "HTTP cookie)。该指令已由指令2009/136进行了修订，其中引入了几项更改，尤其是关于cookie的更改，这些更改现在需要事先获得许可。

据估计，《电子[隐私权法规》](https://en.wikipedia.org/wiki/EPrivacy_Regulation_(European_Union)" \o "隐私权法规（欧盟）)（[ePR](https://en.wikipedia.org/wiki/EPrivacy_Regulation_(European_Union)" \o "隐私权法规（欧盟）)）将于2019年生效，它将废除《电子隐私权指令2002/58 / EC》，并与《[通用数据保护条例》](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation" \o "通用数据保护条例)（GDPR）一起，并规范同意使用cookie的要求并选择出选项。[[1]](https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002" \l "cite_note-:0-1)[[2]](https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002" \l "cite_note-2)[[3]](https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002" \l "cite_note-3)

## EU–US Privacy Shield

*《美国隐私法》*