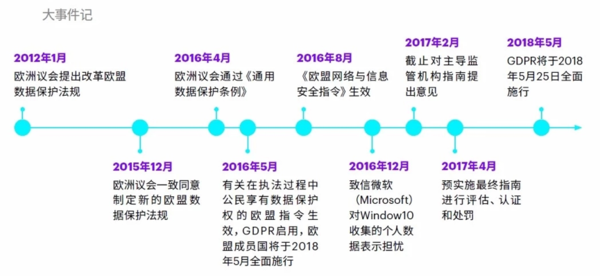
### 什么是GDPR？

2016年4月14日，欧洲议会投票通过了商讨四年的《一般数据保护法案》（General Data Protection Regulation (GDPR)），这项法案赋予欧盟公民更多的个人数据控制权，另外对那些收集、处理和存储个人数据的公司提出更高的责任要求，新法案由11章共99条组成，该法案于2018年5月25日正式生效，将取代现有的《数据保护指令》，统一欧盟成员国关于数据保护的法律法规。GDPR的大部分内容实际包含了“数据保护指令”中既存的理念，但GDPR也引入了一些新的概念，包括针对不合规对象的巨额罚款和增强的数据主体权利。

GDPR作为一套用来保护欧盟普通公民个人隐私信息数据的新法规，对个人信息的保护及监管达到了前所未有的高度，是史上最严格的数据保护法案。



### 适用的范围

1. 适用于设立在欧盟内的控制者或处理者对于个人数据的处理，无论其行为是否发生在欧盟境内；
2. 适用于对欧盟内的数据主体的个人数据处理，即使控制者和处理者没有设立在欧盟内。包括发生在向欧盟内的数据主体提供商品或服务的过程中，无论此商品或服务是否需要数据主体支付对价，或者是对数据主体发生在欧盟内的行为进行监控的。

GDPR适用的数据主体，不仅仅是企业，也包括决定和参与个人数据处理的任何个人、组织，涵盖政府部门、公共组织、司法机构及其他实体。上述个人或实体（除欧盟境内企业及机构，只要涉及向欧盟境内个人提供服务并处理或监控个人数据）作为数据控制者或数据处理者的均在适用实体范围内。

GDPR更多的是监管企业对数据的使用行为，以下4个方面的数据使用情况不适用于GDPR：

1、为了预防、调查、侦查或起诉刑事犯罪，主管当局为执行刑事处罚目的而产生的数据处理行为；

2、基于国家安全目的而产生的数据处理行为；

3、自然人在纯粹的个人或家庭活动中产生的数据处理行为；

4、欧盟法律规定范围之外的活动过程中产生的数据处理行为。

### 涉及哪些个人数据

“个人数据”定义是指任何指向一个已识别或可识别的自然人信息。该可识别的自然人能够被直接或间接的识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线身份认证标识，或者通过参照针对自然人的一个或多个要素（物理、生理、遗传、心理、经济、文化或社会身份）。这意味着GDPR扩大了定义，包括“已识别”和“可识别”的数据信息，已识别个人数据指传统个人数据（姓名、照片、电子邮件、电话号码、家庭住址、身份证号码、银行帐号或社保卡号等），可识别个人的信息是指位置定位数据、移动设备ID以及某些情况下的IP地址、生物特征数据和遗传数据等。

敏感个人数据，是指揭示种族或民族出身，政治观点、宗教或哲学信仰以及工会成员的个人数据，以及唯一识别自然人为目的的基因数据、生物特征数据、自然人的健康、性生活或性取向数据，还包括刑事定罪和犯罪相关的个人资料等。组织应识别其处理个人数据或特殊类敏感个人数据的具体类型。

### 个人数据处理相关的原则

GDPR规定，数据处理是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他的利用，排列、组合、限制、删除或销毁，且无论此操作是否采用自动化的手段。

GDPR规定了个人数据处理的以下基本原则：

1. 合法、正当、透明
2. 处理数据的目的是有限的
3. 仅处理为达到目的的最少数据
4. 确保数据准确、及时更新
5. 存储数据的期限不得长于为达到目的所需要的时间
6. 采取技术和管理措施以保护数据的安全
7. 数据控制者有责任并应能够证明做到了以上几点

### 合法处理数据的定义

GDPR规定，数据处理行为首先应具备合法性基础，GDPR规定的六种合法性情形包括：数据主体的同意、合同 履行、履行法定义务、保护个人重要利益、维护公共利益以及追求正当利益。总结为至少满足以下列举中的一项：

1. 数据主体同意为了特定目的处理其数据
2. 处理数据是为了签订或履行合同的需要
3. 处理数据是为了遵守法定义务的需要
4. 处理数据是为了保护数据主体或其他自然人的至关重要的利益
5. 处理数据是为了公共利益或形式政府授受的权力
6. 处理数据是为了追求数据控制者的合理利益，但不得损害数据主体的利益

GDPR强调同意是指“数据主体通过书面声明或经由一个明确的肯定性动作，表示同意对其个人数据进行处理。该意愿表达应是自由给出的（freely given）、特定具体的 （ specific ）、知情的（ informed ）、清晰明确的（unambiguous）”，且撤回同意的方式应该与表达同意同等便利。组织应保证其数据处理活动满足合法性要求。

### 对儿童数据的特别规定

GDPR在“信息社会服务中适用儿童同意的条件”规定，如果直接向儿童提供信息社会服务时，该儿童的年龄应当为16周岁以上。若儿童未满16周岁，只有在征得监护人同意或授权的范围内其处理才合法。各成员国可以对上述年龄进行调整，但是不得低于13岁。组织如涉及儿童个人数据的处理，应予以特别保护。

### 数据主体的权利

GDPR赋予了数据主体对其数据广泛的控制权，包括知情、访问、更正、删除、限制处理、可携带、反对等权利。 比如：

1. 在数据收集时，数据控制者应以简洁、透明、易懂及便于访问的方式向数据主体提供数据控制者身份及联系信息、数据处理的目的及合法基础、数据主体享有的权利等信息。
2. 个人拥有被遗忘权，当个人数据已和收集处理的目的无关、数据主体不希望其数据被处理或数据控制者已没有正当理由保存该数据时，数据主体可以随时要求收集其数据的企业或个人删除其个人数据。如果该数据被传递给了任何第三方（或第三方网站），数据控制者应通知该第三方删除该数据。GDPR也规定了若干删除权不适用情形，如为行使言论和信息自由的权利，为履行数据控制者法定义务，为设立、行使或捍卫合法权利等等。
3. 数据主体有权拒绝数据控制者基于以下目的对个人数据进行的处理行为，如为公共利益，为数据控制者的合法利益，以直接营销为目的，基于科学或历史研究以及统计目的的数据处理行为等。
4. 数据主体有权在以下情形限制数据控制者的处理行为，如质疑数据准确性，违法处理，数据到期等。
5. 数据控制者基于数据主体同意或履行合同所必须，以自动化方式处理数据主体提供的个人数据时，数据主体有权从数据控制者取得结构化可机读的个人数据副本，并传送给另一个数据控制者。

### 数据控制者与数据处理者的规定

数据处理者是指为数据控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

当数据控制者委托数据处理者具体处理数据时，数据控制者应选择采取了合适的技术和组织方面措施的数据处理者，以确保数据处理符合GDPR的要求，及保障数据主体的权利。在没有数据控制者事先或一般性的书面许可时，数据处理者不应再与另外的数据处理者合作。 组织如属于数据处理者，应根据数据控制者明确的指示处理个人数据，履行相应的保密义务，在数据处理服务结束时，删除或返还所有的个人数据，接受数据控制者的审计等。

可能涉及到以下义务：

1. 设置DPO（数据保护官）
2. 文档化管理
3. 数据保护影响评估
4. 建立事先咨询机制
5. 数据泄露报告机制
6. 安全保障措施
7. 遵守数据跨境转移规则

### 数据泄露强制通知的规定

GDPR规定，在发生个人数据泄露时，除非个人数据的泄露不会产生危及自然人权利和自由的风险，否则数据控制者应在获知泄露之时起的72小时内向监管机构发送通知报告。另外，当个人数据泄露可能对自然人的权利和自由产生高风险时，数据控制者还应当向数据主体告知数据泄露的相关情况。组织应注意如发生个人数据泄露等安全事件，需履行的通报和告知义务。

### 处罚的规定

不遵守信的数据隐私法规的后果就是会受到严厉的制裁和巨额的罚款。

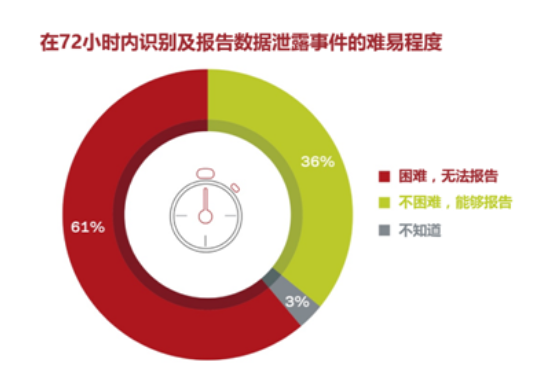
GDPR对违规组织采取根据情况分级处理的方法：

如果组织未按要求保护数据主体的权益、做好相关记录，或未将其违规行为通知监管机关和数据主体，或未进行数据保护影响评估或者未按照规定配合认证，或未委派数据保护官或欧盟境内代表，则可能被处以1000万欧元或其全球年营业额 2％（两者取其高）的罚款。

如果发生了更为严重的侵犯个人数据安全的行为，如未获得客户同意处理数据，或核心理念违反“隐私设计”要求，或违反规定将个人数据跨境传输，或违反欧盟成员国法律规定的义务等，组织有可能面临最高2000万欧元或组织全球年营业额的4%（两者取其高）的巨额罚款。

### 合规的难点

Veritas Technologies近期发布的Veritas 2017 GDPR报告结果指出，在声称符合合规要求的企业中，大约一半(48%)的企业对个人数据并没有全面的可视性，更别提防止个人数据泄露。不仅如此，认为自身企业满足合规的61%受访者承认，自身企业难以识别个人数据泄漏事件，并且无法在72小时以内进行报告。



难以履行被遗忘权

GDPR规定，数据主体有权随时要求收集其数据的企业或个人删除其个人数据。但很多企业应用或服务，无法销毁曾经使用的账户及删除个人信息，无法提供搜索、查找或删除个人数据，甚至无法准确定位显示数据的存储位置，因此无法满足“被遗忘权”的要求。

参考建议：

针对GDPR中的核心要点深度分析国内的企业应该如何应对。这里的应对建议涉及到系统架构、人员管理、流程管理、风险评估、业务逻辑、应急响应等众多环节，以下内容可作为企业自查的一种分析方式。

1. 必须明确询问用户，是否允许同意搜集他们的数据。必须以清晰的方式询问用户，而不能以任何方式默认用户授予开发者数据使用许可权。

如下的询问是明确的（符合GDPR要求）：

点击下面的按钮，表示您同意收集您的个人数据并用来推荐相关的信息/广告；

点击下面的按钮，表示您不同意收集你的个人数据；

如下的询问是不明确的（违反GDPR要求）：

以复选框的形式呈现，默认勾选『同意收集数据用于…』；

请阅读下面的关于GDPR的条款（然后要求用户勾选『我同意上述的条款』）。

2．提供自助登录入口，可供查询、更新个人信息；提供账户销毁/删除功能，确定服务或协议终结，可允许选择销毁账号及信息，并删除一切有关个人数据，包括第三方账户登录（可以通过加密数据，然后删除密钥）。

3．需要强密钥管理以保护加密的数据，合理区分数据控制者和数据处理者，对权限和身份进行合理划分。

4．识别数据存储的位置（特别需要注意云计算服务资源），数据的类型及风险级别，严格把控信息数据的访问控制。

5．遵守“知其所需”（Need to know）原则，只收集所需要的最少个人数据，并采取技术和管理措施来保护数据的存储安全和传输安全，避免个人数据被篡改、丢失、未经授权披露或被恶意攻击。

6．设置专门的隐私保护人员，实施问责机制；建立数据生命周期管理，定期更新或销毁，定义流程及描述以对数据泄露做出敏捷反应。

7．建立内部隐私管控制度，并与专业安全服务公司保持联系。

8．进行全面的风险评估；应用关键安全控制来恰当地检测、管理和缓解数据处理环境中的任何漏洞；根据企业策略配置系统，并维护该配置；持续监视日志文件，警惕任何潜在数据泄露或漏洞。

关于欧盟 GDPR 原文，参见：

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv :OJ.L\_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

全国信息安全标准化技术委员会秘书处发布《网络安全实践指南——欧盟GDPR 关注点》

<https://www.tc260.org.cn/upload/2018-05-25/1527251794595094938.pdf>