德勤企业风险 第六辑

个人信息保护——
应对法律合规要求，妥善处理个人信息

德勤企业风险管理服务部　编

Deloitte.
德勤

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

德勤企业风险（第六辑）

个人信息保护
——应对法律合规要求，妥善处理个人信息

德勤企业风险管理服务部 编

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内 容 提 要

本书是德勤企业风险丛书的第六辑，主要涉及个人信息保护的最前沿话题。内容包括如何通过数据丢失防护系统应对日益严格的信息保护法规及监管要求；个人信息保护立法及监管要求；个人资料保护制度建置；隐私保护的企业现状和合规挑战；管理数据隐私的利器——身份和访问管理；个人资料泄漏调查经验；企业敏感数据保护之道；银行信息科技安全风险管理探讨，等等。本书可为企业的个人信息保护提供理论基础和最佳实践。

本书适合企业管理人员、相关政策制定者以及研究者参考阅读。

图书在版编目（CIP）数据

个人信息保护：应对法律合规要求，妥善处理个人信息 / 德勤企业风险管理服务部编.
—上海：上海交通大学出版社，2013
（德勤企业风险．第6辑）
ISBN 978-7-313-09784-2

Ⅰ．①个… Ⅱ．①德… Ⅲ．①隐私权-法律保护-研究 Ⅳ．①D913.04

中国版本图书馆CIP数据核字（2013）第111772号

个人信息保护
——应对法律合规要求，妥善处理个人信息
德勤企业风险管理服务部 编
上海交通大学出版社出版发行
（上海市番禺路951号 邮政编码 200030）
电话：64071208 出版人：韩建民
上海华业装潢印刷有限公司印刷 全国新华书店经销
开本：890mm×1240mm 1/16 印张：4.75 字数：130千字
2013年6月第1版 2013年6月第1次印刷
ISBN 978-7-313-09784-2/D 定价：30.00元

德勤企业风险
德勤企业风险管理服务部 编

编委
刘伟杰
蒋黎虹
薛梓源
黄皓礼
陈嘉祥
林允纲
方　烨
谈　亮

执行编委
原国太郎
孙永杰
冯文珊
彭为德
赵　理
何　萍
庄宇杰
吴坚隽

编委助理
李　华

前言

"O, wonder! How many goodly creatures are there here! How beauteous mankind is! O brave new world, That has such people in't!"

——William Shakespeare, The Tempest, Act V, Scene I

“神奇啊！这里有多少好看的人！人类有多么美丽！啊！美丽的新世界，有这样的人在里头！”

——威廉·莎士比亚《暴风雨》第五场，第一幕

随着经济的迅猛发展，科技的力量越来越大，沟通的方式越来越多，资讯的传播越来越自由，人与人的距离越来越近。生活在这个愈渐狭小的地球村，人与人之间的信息交流与传播似乎轻而易举，让我们能生活在这美丽的新世界 (O brave new world, That has such people in't!) 。然而在这看似自由发达的外表下，信息安全及隐私泄漏的问题却无孔不入地渗入人们的生活。

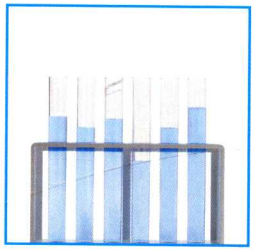
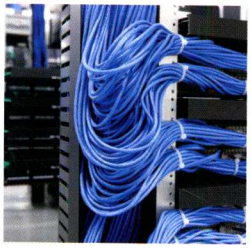
繁多的资讯传播途径给人们的生活带来众多便利，个人的隐私却在这样的环境下无所遁形。移动电话号码、网上银行密码、公司内部决策等，这些私密信息随时都有可能被利用、误用，甚至被盗用和滥用，导致人们隐私的暴露，公司机密的泄漏。这种将隐私公之于众的行为不仅给个人带来身心的伤害，更会导致公司名誉受损，业绩受创。

为了遏制隐私泄漏这一电子信息高速发展下的衍生物，国家政府机构及相关团体已出台相关法律法规，以保证个人隐私不被侵犯。德勤作为行业的先驱，凭借自身专业的知识和多年的经验，有责任创造一个安全的信息环境，一个隐私受保护的时代。当人们可以在这电子化的时代里真正享受科技发展和信息分享的好处时，他们定能由衷地赞叹：

“神奇啊！这里有多少好看的人！人类有多么美丽！啊！美丽的新世界，有这样的人在里头！”

顾向圣
大中华企业讯息管理主管
企业风险管理服务合伙人

目录

如何通过数据丢失防护系统（DLP）应对日益严格的信息保护法规及监管要求？

谭锐坚　总监
德勤香港事务所
企业风险管理服务

近年，传媒经常报道有关机构泄漏机密信息和滥用个人信息的情况。例如，在零售商店的会员制度中，客户提供的个人信息被过度收集；另外，有金融机构在没有获得客户同意的情况下，与第三方共享客户个人信息作直接促销用途；以及有医疗机构曾经遗失了载有病人病历记录的U盘，继而导致资料外泄。很显然，被指控的机构因此对自己的声誉造成负面影响，最终可能会因为机构和客户之间缺乏信任而影响了他们的经营业绩。

以上个案使得大众的注意力转向机构如何保管机密信息和保存他们的个人信息。他们会质疑机构是否有任何有效和足够的控制，以保护这些信息的安全，从而避免未经授权的访问和使用不当的情况发生。

另一方面，机构可能也注意到大众对机构如何保护他们提供给机构的个人信息的关注。为了提供足够的信息保护，机构可能会考虑这样的问题：机构可否确保在有需要的时候提供适当的数据？机构可否控制数据的访问权限？机构可否保护数据，防止机构内部/外部的信息被盗窃？机构可否遵从相应的法律要求（如《隐私法》）来保护客户数据？机构是否正确保护信息管理的基础设施？机构可否采用新兴技术（如云计算和移动计算）？

一、信息保护的法规/监管要求

在信息保护的重要性在全球上升的同时，来自不同国家的政府及监管机构已推出了各自的信息保护条例，并已在自己的国家中实施。在亚太区中，一些国家和地区如新加坡、菲律宾、韩国、印度尼西亚、泰国和日本等近年都制定了自己的信息保护原则，并已在几个主要范围上作出限制和指引。包括获取信息的应用、信息采集及处理、信息的传输以及违例通知，等等。

(一) 香港的《个人资料（私隐）条例》(PDPO)

早在1996年12月香港就已经通过并实施了一套名为《个人资料（私隐）条例》的法例，用以确保每个人的个人信息得到保护。《个人资料（私隐）条例》是香港首套信息保护和管理的法定条例。它主要可以概括为以下6个信息保障的原则：

(1) 个人资料的收集必须与资料使用者的职能和活动有关，而收集的资料适量便可及以合法及公平的手法收集，并须告知收集的目的及资料的用途；

(2) 须采取切实可行的步骤确保个人资料的准确性，并在完成资料的使用目的后，删除资料；

(3) 限制个人资料使用于当初的收集目的或直接有关的用途上，否则必须先获得资料当事人的同意；

(4) 须采取切实可行的步骤确保个人资料的安全，免受未获授权或意外的查阅、处理、删除、丧失或使用的影响；

(5) 制订及提供个人资料的政策及实务；

(6) 个人有权查阅及更改个人资料。资料使用者应在指定的时间内依从查阅或更改资料的要求，除非条例订明的拒绝理由适用。

(二)《个人资料（私隐）（修订）条例》(PDPAO)

电子商务以及相关技术的快速发展，引致全球对信息保护及隐私的关注。为了配合形势，香港进行了《个人资料（私隐）条例》的检讨，分析当时现行的法规对保护个人信息的充分性，并于2012年6月在立法会上通过了《个人资料（私隐）（修订）条例》。

《个人资料（私隐）（修订）条例》修改了个人数据（私隐）条例的原有条文；尤其是把信息用作直接营销的机构，严格规定了该类机构对个人信息的使用的限制，特别是这样的信息的提供和销售。

1.机构在直销方面的责任

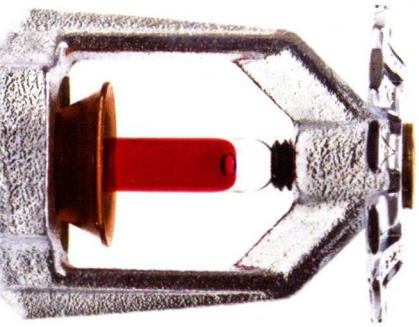
在机构使用个人资料做直销前，须告知信息当事人，在取得其同意后方可使用其个人资料。而机构亦须明确告知信息当事人以下信息：拟使用个人资料的种类、该资料被用于何种类别的促销标的、提供途径，让当事人传达同意或不同意。如果机构希望把相关信息转移给第三方，则除了上述的项目以外，还须以书面形式提供该信息，并告知在信息转移中是否牵涉任何金钱利益的有关事项。

2.外包个人信息处理

当机构请求信息处理方对信息进行处理时，不管处理方是在香港或香港以外的地方，原机构应该与信息处理方签订一份合同以防止传输的信息保存超过所需的时间。合同条款也应防止由意外导致的未经授权的访问或更改（如删除），或信息丢失和未经授权的修改。

3.违反《个人资料（私隐）（修订）条例》的刑罚

至于刑罚方面，如果违反了《个人资料（私隐）（修订）条例》，由于得到信息当事人的同意在条例中是最为重要的一个实际步骤，因此处罚主要根据这一项目而设立。如机构在



没有得到信息当事人同意的情况下披露个人信息，根据该条例，这是一个新的刑事罪行。触犯者可以被处以最高罚款达港币50万元及监禁长达3年。此外，如果信息在没有获得信息当事人授予的有效同意下被“售卖”给第三方，触犯者会被罚款港币100万元及最高刑罚为监禁5年。

(三) 中华人民共和国国家标准（国标）

中国国家标准化管理委员会亦于2013年2月1日实施了中华人民共和国国家标准，该法规旨在治理和保护个人信息的使用。其中的原则覆盖了将所有或部分个人信息输入到信息系统的过程。它适用于所有组织和机构以外的有公共管理职责的政府部门或类似机构。国标还指出，个人信息可以分为个人一般信息和个人敏感信息，并引入默许和明确同意的概念。国标也列明了机构收集和使用信息的8项基本要求，包括：

(1) 须清楚告知信息当事人使用信息的目的；
(2) 收集的信息不可超过必要的范围；
(3) 明确披露收集信息的目的；
(4) 须征得信息当事人的个人同意；
(5) 确保信息质量保证；
(6) 确保信息获得保护；
(7) 执行诚信；
(8) 须清楚界定明确责任。

在国标中，对用户的信息、信息当事人及第三方监测机构的角色进行了明确规定。包括信息当事人的权利、机构的责任、信息持有者删除信息的责任和第三方监测机构的基本成效。它也清楚地定义了信息处理周期的顺序，并将其依次分为4个阶段：信息收集、信息处理、信息传输和信息删除。

此外，国标有八大原则，用以标出重点领域范畴，当中包括：

(1) 目的明确原则。处理个人资料要有特定、明确、合理的目的，不扩大使用范围，不在个人资料主体不知情的情况下改变处理个人资料的目的；

(2) 最少够用原则。只处理与处理目的有关的最少资料，达到处理目的后，在最短时间内删除个人资料；

(3) 公开告知原则。对个人资料主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人资料主体告知个人资料的处理目的、个人资料的收集和使用范围、个人资料的保护措施等；

(4) 个人同意原则。处理个人资料前要征得个人资料主体的同意；

(5) 品质保证原则。保证处理过程中的个人资料保密、完整、可用，并处于最新状态；

(6) 安全保障原则。采取适当的、与个人资料遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人资料安全，防止未经个人资料管理者授权的检索、披露及丢失、泄露、损毁和篡改个人资料；

(7) 诚信履行原则。按照收集时的承诺，或基于法定事由处理个人资料，在达到既定目的后不再继续处理个人资料；

(8) 责任明确原则。明确个人资料处理过程中的责任，采取相应的措施落实相关责任，并对个人资料处理过程进行记录以便于追溯。

二、机构面对信息保护方面的挑战

如今，许多机构已经实施了监控系统来识别机密信息和传输过程中的信息交换，以防止信息丢失。然而，这些措施仍然可能存在一些漏洞，如监控系统可能无法正确识别机构的机密信息，或者它是否能适当地为机密信息进行加密，这仍然是一个值得机构认真考虑的重点。

机构的个别员工也可能被其他人提供的一些好处所引诱，而有意或无意地泄露了相关的个人信息，而那些人则将该信息用在非法的用途上。例如，将一个包含间谍软件的电邮或U盘存入电脑以获得一个抽奖机会或赢得购物优惠券，等等。人们很容易因为未察觉而掉进这样的陷阱，从而被欺骗并无意地泄漏了信息。

三、数据丢失防护系统(DLP)

在过去的几年中，机构的日常业务运作对电脑系统的依赖日益增长，大量的信息传输是十年前所无法比拟的。加上信息系统的复杂性不断增加，数据丢失或泄漏信息的风险比过去更容易发生。

对于任何机构，数据泄漏/亏损都是不可接受的，因为它往往会导致机构受到财务及声誉/公信力的损害。在丢失/泄漏敏感数据的情况下，机构甚至面对诉讼的可能性。

为了防止发生上述损失，机构可以部署数据丢失防护系统（DLP）政策。它通常是机构按照自己的政策和地方/区域法制定的战略和软件的结合。机构要保护信息，有效的DLP是必要的，因为它涵盖了大多数类型的信息丢失，无论它们是有意、无意（人为错误、错位）或犯罪（盗窃、黑客、机构未经信息当事人同意向第三方销售信息）。

(一) DLP如何协助保护数据

大多数DLP政策会根据资料的状态用特定的软件和方法，通过检测和监测三种主要类型的信息，来实现信息保护。

第一类是传输中的信息（Data in Transit）。它包括进、出或流通于组织内部数位化平台的信息。特定的软件会被整合到机构网络去跟踪内部网络的网络运动或任何可疑的网络交通。通过使用深度包检测(DPI)技术，能够选择性地扫描网络中的信息包内容及它们的源头、目的地和流量。要实现这个功能，传输中的信息应该事先解密或软件有能力去解密，检查后再对其进行加密并传送。如果检测到任何未经授权或不符合机构安全政策的信息传输，DLP软件应能够立即停止有关传送并通知发件人的上级。

第二类是使用中的信息（Data in Use）。这比其他两类信息更加难以监控，因为它包括所有电脑内正在使用的信息。例如将信息复制到一个USB驱动器，将信息发送到打印机，甚至是应用程序之间的信息传输。通过软件代理（Agent）设立的规则，DLP可以保护这些信息，迫使用户遵从并限制他们的权利，其中可能包括防止复制信息时终端机未连接到内部网络或阻止用户试图复制敏感信息到U盘。

第三类是闲置信息（Data at Rest）。此类型通常需要一种名为Crawler的软件在机构的数据库中搜索和定位特定信息及档案类型，无论它们是电脑、储存局域网络还是档案存储的信息。Crawler会打开这些档案，并确定它们所包含的敏感信息，然后评估信息是否被放置在中央管理层事先定下的安全规则水平内一个合适的路径。机密信息，如信用卡信息，将被放在安全的路径中并被加密，以防止任何未经授权的访问或活动。此外机构应该定时创建信息备份，以防止可能的硬件、软件故障，停电事故和自然灾害产生的任何信息损失等。

政策方面应设立拥有系统许可权的特权用户，以确保只有选定的个人才可以改变机构的DLP解决方案的设定。最理想的人选就是中央管理层，因为他们更了解日常业务中传输敏感信息的必要性，并对相关政策提出更改，而且发生问题时更容易追究责任。为了避免中央管理层的权力过大，机构必须制订相关政策，防止他们在犯下罪行的同时隐瞒犯罪（例如出售客户个人资料）。提高对信息保护的认识，为员工提供培训，也是DLP的一个非常重要的部分，由于大多数信息丢失事件的发生是由于人为错误，给予他们相关知识亦能减少此等错误和信息损失。

(二) 实施DLP解决方案的优点

通过实施有效的DLP解决方案，机构对本地/区域规则和法规的遵守将得到改善，可减少违法和面临诉讼的可能。DLP的另一个好处是，在检讨和测试当前的业务流程中，任何不必要或错误的过程均会被发现。促使中央管理层制订一个解决方案，从而进一步降低安全性漏洞的产生，更好地保护敏感信息，避免任何不必要的信息丢失或泄漏。再者，通过浏览机构的储存服务器和网络带宽，DLP可以识别任何不必要的信息，删除它们并降低备份所需的大小，从而优化磁盘空间和带宽。

(三) 实施DLP解决方案要考虑的要点

首先，DLP不是万能的，它有它的限制。例如，无法全面解读所有格式的档案内容，图片上的敏感信息或设计档案可能不能被全面侦查及拦阻；移动设备也较难被监测和控制，因为它们有能力发送短信，拍下照片并录制影像档案。因此随着软件的使用，机构必须制定相应的规则和法规，以提高员工对保护信息安全的重要性和损失信息的严重后果的认识。正确运用适当的规则、法规与软件，能进一步将信息丢失的风险降到最低。

由于DLP软件主要是通过制订规则去执行相应的职责，决策规则过于严格或宽松都将使DLP解决方案的效用降低。若没有正确实施机构的解决方案所需的合适的规则，DLP也可能会带来业务操作上的风险。例如传输中的敏感信息未被成功侦查或其他非敏感信息被过度拦阻。为了尽量减少此类风险，机构的管理层必须制订有关的DLP信息保护规则和业务操作流程，并在需要时雇用专家顾问协助。通过制订并实施有关的规则和业务流程，以实现信息保护的最佳实践。

个人信息保护立法及监管要求

何晓明　副总监
王　婧　经理
德勤北京事务所
企业风险管理服务

伴随着中国经济的飞速发展和科技的巨大进步，信息时代真正地来到每个人的身边，信息的含金量及其对日常生活的影响日益彰显，为提供定制化的客户服务以提高客户服务满意度，客户的身份、家庭、财务状况等个人信息成为服务提供者需要掌握的基本信息，客户在享受服务提供者提供的量身定制服务的同时，也逐渐注意到，一些推销和诈骗电话对自己的信息了如指掌。此外，由于个人信息泄露导致的信用卡盗用事件的相关报道也不绝于耳，甚至不乏一些人身安全事件。如此诸般，立法机关、行业主管部门、社会媒体等各方力量，越来越多地提到个人信息保护的重要性，也催生了一系列法规及指引的出台。中央电视台2013年3.15晚会曝光的安卓系统第三方应用开发者在未经用户授权的情况下对用户个人信息进行采集，收集了大量用户个人信息的事件，实际上只是以个人移动通信终端为触点，揭示了当前媒体、公众以及个人用户等各方对于个人信息保护的日益关注，事实上，中国政府和监管机构对于个人信息保护监督力度也在逐步加强。

国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

——《全国人民代表大会常务委员会关于加强网络信息保护的决定》（以下简称《决定》）

一、国家关于个人信息保护的立法

2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议审议通过的这一决定，为加强公民个人信息保护、维护网络信息安全提供了法律依据。为配合《决定》的落实，在具体的指南方面，《信息安全技术公共及商用服务信息系统个人信息保护指南》（以下简称《指南》）作为我国首个个人信息保护国家标准，也已于2013年2月1日起正式发布实施。此文件属国家标准“指导性技术文件”类，与从制度上进行监管的《决定》相比，该《指南》侧重于从技术手段、信息系统上进行监管，对利用信息系统处理个人信息的活动起指导和规范作用，目的是为了提高企业的个人信息保护技术水平，促进个人信息的合理利用。

除此之外，在《决定》出台以后，各部委也开始制定更具体的个人信息保护的相关规定。工业和信息化部起草了《电信和互联网用户个人信息保护规定(征求意见稿)》、《电话用户真实身份信息登记规定(征求意见稿)》（以下简称《规定》），并且已经向社会公开征求意见。根据《规定》，电信业务经营者、管理机构及工作人员不得出售或者非法向他人提供电话用户真实身份信息，否则可以处1万元以上3万元以下罚款，构成犯罪的，依法追究刑事责任。

电信行业《规定》的迅速出台，表现了工信部对于个人信息保护的坚决态度和长期以来的渴望。随着电信行业打响了个人信息保护的“第一枪”，我们有理由相信，其他拥有大量用户信息的行业，也将逐步打响保卫个人信息之战。

二、个人信息保护的需求及《指南》概述

造成个人信息泄露有多种因素。首先，随着网络的进一步发展，个人信息的价值越来越高。巨大的利益驱动，使得不法分子铤而走险。然而，中国公众目前对个人信息的保护意识不强，给犯罪分子留下了可乘之机。并且我国一直以来缺乏明确的法律法规，对个人信息的收集和使用到底怎样是合法，怎样是不合法并没有明确的定义。同时，对于明显的个人信息非授权收集或流转，也没有足够的惩处力度以震慑此种行为。总体来看，在个人信息处理流程中，个人信息非授权采集和个人信息第三方流转是个人信息保护的两个主要风险点。《指南》分五个章节，分别描述了个人信息保护的范围、参与对象和相关方的定义、角色和职责以及信息处理阶段的具体标准。在该《指南》中对个人信息的类别、信息相关方的类别和信息处理的环节都进行了明确的区别和划分。

(一) 个人信息

《指南》最显著的特点是将个人信息分为个人一般信息和个人敏感信息，并提出默许同意和明示同意的概念。对于个人一般信息的处理可以建立在默许同意的基础上，只要个人信息主体没有明确表示反对，便可收集和利用。对于个人敏感信息，则需要建立在明示同意的基础上，在收集和利用之前，必须首先获得个人信息主体明确的授权。

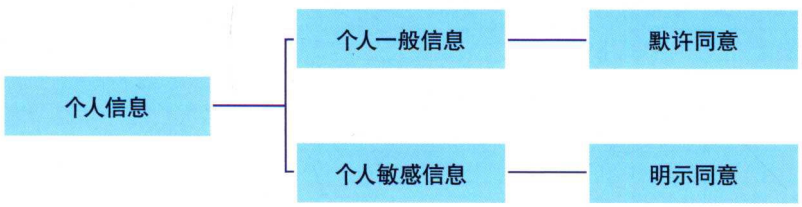


图1 个人信息的分类

(二) 信息相关方

《指南》将信息相关方分为个人信息主体、个人信息管理者、个人信息获得者和第三方测评机构。

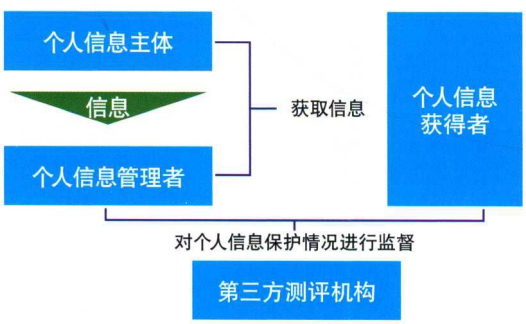


图2 信息相关方

(1) 个人信息主体。个人信息指向的自然人，信息的真正所有者。

(2) 个人信息管理者。决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

(3) 个人信息获得者。从信息系统获取个人信息的个人、组织和机构，依据个人信息主体的意愿对获得的个人信息进行处理。

(4) 第三方测评机构。独立于个人信息管理者的专业测评机构。

(三) 信息处理

《指南》将个人信息处理分为收集、加工、转移和删除四个主要环节，对个人信息的保护贯穿于四个环节中。

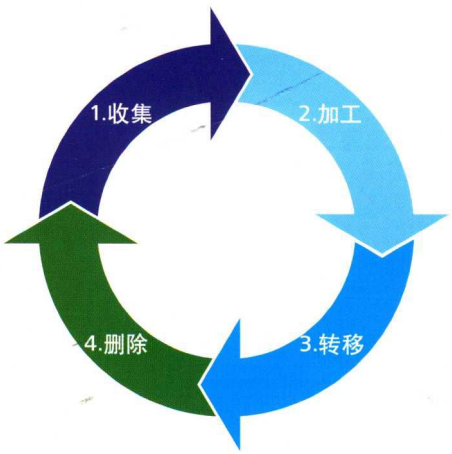


图3 个人信息处理的主要环节

(1) 在收集阶段，要求目的合法且告知个人信息主体。

(2) 在加工阶段，要求将加工目的及方法等告知个人信息主体。

(3) 在转移阶段，要求告知个人信息主体转移的范围和目的。

(4) 在删除阶段，要求收集阶段告知的个人信息使用目的达到后，立即删除个人信息。

从以上四个环节的要求来看，《指南》主要强调的是个人信息主体的“知情权”，要求对于个人信息的处理全部要告知个人信息主体，且处理不能超出告知范围。这项标准还提出了处理个人信息时应当遵循的八项基本原则，即目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确。

该《指南》为下一步有针对性地打击相关犯罪提供了有力武器。但是，这个《指南》仅是一个技术性标准，缺乏对违反这个标准的惩罚性措施，因此对于打击个人信息犯罪尚不具有威慑性。在网络上保护公民权益免受非法侵害、保障国家安全是一项系统工程，不是单靠一部法律、法规就可以完成的。制定具有可操作性的法律必不可少，但要想从根本上解决个人信息泄露的问题，还需要不断完善相关的网络法律法规，建立健全相应的配套制度。

总体来看，我国在个人信息保护立法方面还处于初级阶段，虽然出台了标准并准备颁布法案，但具体法案的实施，细则的补充以及实施还需很长一段时间。

三、个人信息保护主要风险点的应对

结合我国国情，目前应对个人信息保护风险，主要需要国家完善立法、民众提高个人信息保护意识和企业规范信息使用三方面的努力。

(一) 在国家立法层面，逐步完善国家立法，尤其是加大个人信息相关违法行为的惩处力度，是应对个人信息第三方流转的有效手段之一

其主要目的是提高相关违法行为的犯罪成本，从而对违法人员起到震慑作用，减少此类行为的发生。我国目前各地政府已开始纷纷“试水”，用实际行动立法保护个人信息，如湖北、湖南、江苏等一些地区，对非法泄露、复制及倒卖个人信息的非法者，处以最高50万元的罚款。随着《决定》和《指南》及一系列具体措施的颁布，对个人信息相关违法行为的惩处力度及范围与日俱增，构成犯罪的，也将依法追究刑事责任。

(二) 在公众防范层面，为防范个人信息的非授权采集，需要提高用户的自我保护意识

作为信息的所有者，个人应采取措施对自己的信息进行保护，包括了解个人信息的范围、个人信息保护的原则和可采用的具体措施。姓名、身份证号、电话号码、住址、账号等可以定位到个人的信息都属于个人信息的范畴。

个人在向外界提供个人信息时，应了解对方获取此类信息的原因，并据此判断对方要求取得的信息是否多于实际需要的信息。坚持“最小够用”的原则，只给对方提供必要的信息，避免在不正规的网站、电商留下个人信息。

在提供信息时，应采取措施限定或表明此类信息使用的范围。例如，在提供身份证复印件时，应在不影响复印件使用的情况下，注明该身份证复印件的用途或授权使用人；在网站注册输入信息时，应关注网站是否提供隐私保护政策，限定信息保密要求或限定使用范围。

在处理包含个人信息的介质时，应采取恰当措施销毁信息。常见的信息介质包括：个人简历、快递单、银行业务凭条、刷卡记录等，在弃置此类介质前应保证个人信息不会被获取，可以采用撕毁、涂画等方式保护个人信息。

除个人要加强信息保护外，政府在加强立法保护的同时，还应加大对个人信息保护的宣传力度，借助广播、电视等多媒体，营造良好的舆论氛围，提高全民的信息安全意识。同时，建立个人信息保护制度的奖励机制，鼓励公众举报侵犯个人信息的违法行为，以便从源头上找到真正的元凶。

(三) 在企业层面，出于控制声誉风险和法律风险的角度，企业需加强对个人信息的保护

随着立法和监管力度的加强，企业也需要加强对于个人信息保护的关注，严格遵守与个人信息相关的合规要求，包括信息收集及使用规范、安全保障措施和监督及检查等方面，并接受与配合相关机构的监督与检查，尽量避免由于个人信息相关违法行为导致的法律责任追究。

同时，从企业声誉风险的角度来看，客户群体对自身信息保护的意识和重视程度都在逐步提升，众多信息泄露事件的曝光和各类传媒对此类事件的持续关注，都对企业声誉风险的控制形成了越来越大的压力。出于对客户群体的负责，以及自身品牌的维护，企业都有必要加强对个人信息的保护力度。

企业在使用用户信息时应关注用户信息泄露的两个主要途径，包括内部泄露和外部泄露。

(1) 内部泄露。主要有员工泄露（例如2012年3.15晚会有相关报道，系统管理人员批量出卖用户数据）和非法外来人员泄露（例如商业间谍等）。

(2) 外部泄露。主要途径是在和第三方合作的过程中，用户信息在企业不知情的情况下被第三方获取（例如信用卡短信提醒功能的短信平台提供商，存储银行的用户手机号码）。

由于用户信息收集、加工、转移和弃置的过程中都存在信息泄露的风险，因此企业应建立全流程、多层次的用户信息保护体系，因为：

(1) 一个完整的用户信息保护体系，可以覆盖可能存储信息的管理对象、信息使用管理的全流程，以及信息保护的相关方。

(2) 一个合理的用户信息保护体系，可以兼顾职责分工、管理流程和技术平台，保证执行人、工作内容和操作工具的高度一致。

(3) 一个灵活的用户信息保护体系，可以通过对每个局部领域的深入和细化，制订可落地实施的管控措施。

企业在个人信息保护中应全面考虑信息收集、加工、转移和删除环节的风险，应梳理个人信息在本企业使用过程中的全部流程，包括涉及的系统和外包商、合作伙伴，逐一评估流程环节中个人信息泄露的安全风险、客户通知的合规风险、事件处理的声誉风险等。

企业在收集、使用个人信息时，应至少做到：

(1) 小范围、先认可。在收集环节，只收集必要的个人信息，并根据个人信息的性质，获得信息主体的认可。

(2) 防泄漏、透明化。在加工环节，采取必要措施防止数据泄露，并向信息主体告知加工目的和方法。

(3) 不放松、广告知。在转移环节，对外包商和合作伙伴应要求采取与企业自身管理一样的安全管理要求，保证在个人信息使用的过程中不出现管理的短板，并明确告知信息主体转移的范围和目的。

(4) 及时删、不保留。在删除环节，当使用目的达成后，及时删除个人信息，包括企业自身保存的，以及外包商和合作伙伴保存的数据。

综上所述，企业在管理个人信息时，除做好自身安全管理，关注外包商和合作伙伴的安全水平之外，还要体现对信息主体的尊重和负责，保障信息主体对个人信息使用情况的知情权。

个人资料保护制度建置项目经验谈

吴佳翰　合伙人
曾　韵　高级经理
游靖芬　副经理
德勤台北事务所
企业风险管理服务

许多机构初次听到有新版《个人资料保护法》时，都会问：“我们还要多做什么？”了解法规的内容以后，不禁哀鸿遍野：“这太严格了！对我们的业务执行将造成很大影响！”而那些以往未曾被《电脑处理个人资料保护法》规范的行业，更是惊恐：“罚则这么严？到底应该怎么做才不会被罚？我们连从何开始执行的头绪都没有！”这些冲击都始于2011年5月26日正式公布新版《个人资料保护法》之时，全台湾不管是公务机构或非公务机构都开始“疯”行个人资料保护，并被深深地困扰着。

新版《个人资料保护法》参考APEC隐私保护纲领，各行各业都将受到新规范的影响，即便是过往已遵循《电脑处理个人资料保护法》的产业，其遵循程度仍不够彻底。综观亚太其他地区（如中国香港、日本与韩国等），其个人资料保护的法令进程与个人资料保护意识均较台湾成熟，对于台湾即将面临的个人资料保护的挑战，或可作为借鉴参考。

德勤在研究了台湾与各地的个人资料保护相关法令法规以及国际标准要求，并融合各产业的个人资料项目经验后，对于个人资料保护机制提出“五个方面与七个步骤”，作为执行个人资料保护的参考。五个方面是：①组织本身；②委托机构；③当事人权利；④预防机制；⑤事后应变（见图1）。七个步骤是：①制订法令基准；②盘点个人资料；③了解风险程度；④设计管理机制；⑤确实遵循机制；⑥进行机制核查；⑦持续矫正预防（见图2）。

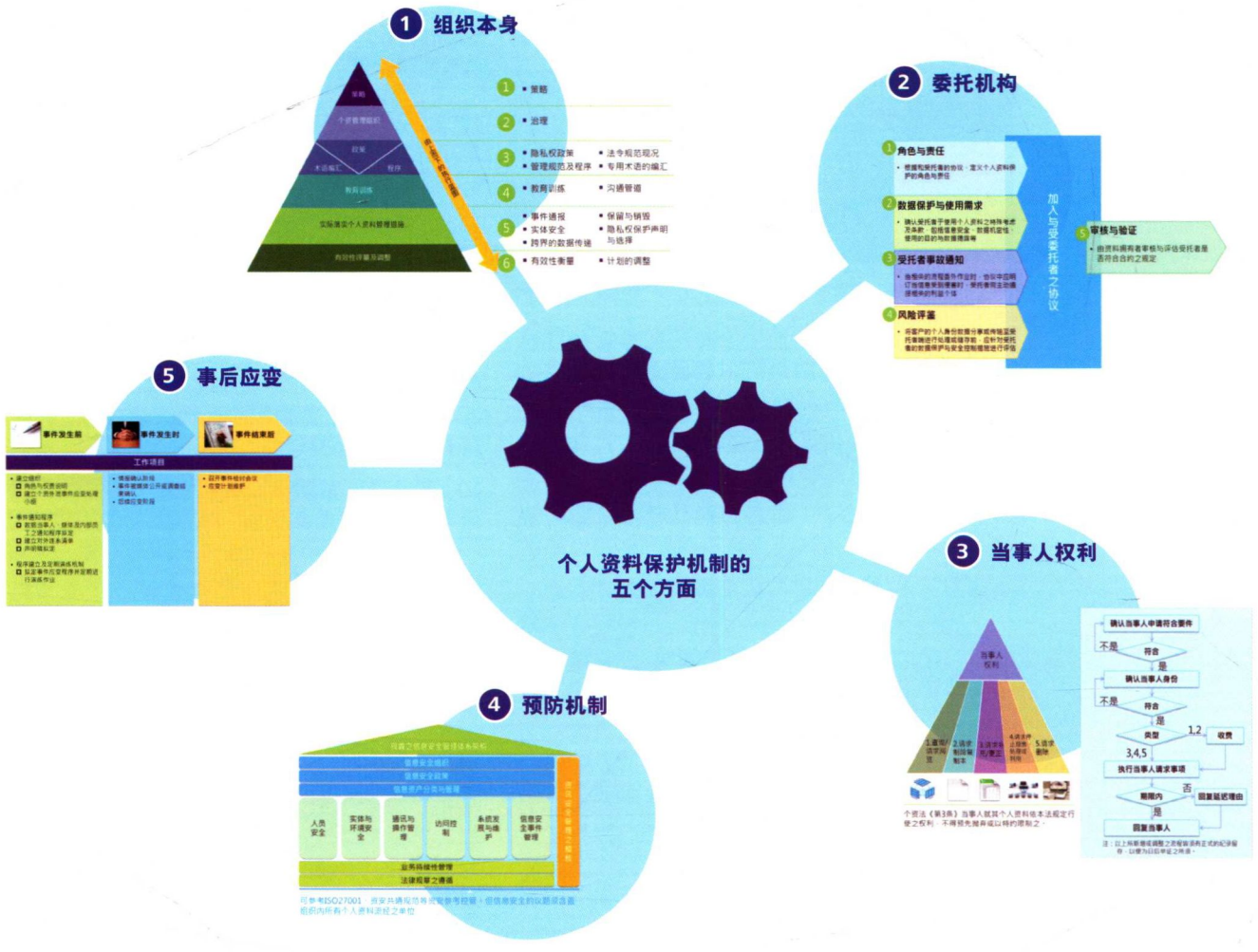


图1 个人资料保护机制的五个方面

图2 个人资料保护机制的七个步骤

各产业因其特性不同，对于新版《个人资料保护法》的规范的确会有窒碍难行之处，以下提出各产业可能面临的冲击。

金融业以往有许多间接搜集个人资料的情况(如信用卡申请书上除申请人的资料外还有其他联络人的信息)，若都要在《个人资料保护法》实行后一年内完成告知，则告知将耗费巨额成本。此外，若考虑删除此间接搜集的个人资料，部分以特殊形式存在的个人资料(如图像文件)则难以完全辨识与删除。

无实体店面的产业在搜集个人资料时以网页形式达成契约关系，并在网页中进行告知作业，但如遇特定目的外的利用时，《个人资料保护法》又规定必须获得当事人的书面同意，故业者往往需要以实体信件寄给当事人以获得同意，或是建立一套符合数字签名原则的身份认证机制，而这皆需耗费高额成本。

以上的两个例子仅是冰山一角，新版《个人资料保护法》已取消行业的限制，各行各业均会受到冲击，在遵法的议题中，不管法律制定的宽松程度如何，法令遵循与业务收益之间的冲突是难解的议题。

在企业进行个人资料保护的作业时，还有另一个难解之题，即个人资料保护的治理架构。在台湾《电脑处理个人资料保护法》的时代，个人资料保护的议题理所当然被认为属于资讯部门，然而新版《个人资料保护法》公布后，此议题将涉及企业内所有可能接触到个人资料的部门，基本上就是企业内的所有部门。如何把负责个人资料保护作业的权责拓展至各部门，并找出一个主持大局，统筹各部门的人或组织来推动个人资料保护亦是一门学问。只要企业的个人资料保护角色权责能够明确，推行个人资料保护即会事半功倍，并一路顺畅。

若企业了解了法令，明确了个人资料保护的组织，接下来面临的问题就是找出个人资料。大部分企业的问题在于不能明确地辨别哪些是个人资料，或存在个人资料遗漏的不安全感，这些问题都是因为个人档案会在组织内流动而非静止，各部门若是各自盘点个人资料，势必会有漏缺的情况。盘点个人资料，除了须花费时间、人力资源外，盘点的方法也非常重要，好的方法可以让盘点过程更完整、更顺利。

虽说个人资料保护是合规的议题，但信息安全的部分亦不容忽略。举例来说，个人资料进行传输时，为了保护其机密性，可以将其压缩并加密，再用电子邮件进行传输；而以电子文件形式存在的个人资料在删除时，为了使其消失不复存在，可以使用Shift+Del进行删除。但上述的两个案例都不是绝对的，对于安全控管的议题，并没有标准答案。所以企业常会问：“要买什么产品才可以达到保护个人资料的目标？”、“这样的保护程度就足够了吗？”企业常会质疑，科技产品日新月异，到底要使用何种新颖的防护设备才能防止个人资料受侵害，而旧的产品是否都要淘汰？如果盲目地追逐新技术，则企业要付出的成本将永无止境，但不这样做，合规的风险又会很高。建议企业应落实个人资料管理风险分析与评估作业，在设计控管与资源提供时，必须彻底了解自身情况，理性地找到平衡点。

最后，所有的企业都会问一个问题：“实施了所有的个人资料保护措施，个人资料就不会外泄了吗？”或者是进一步问：“如果都做了，个人资料外泄时还会被罚吗？”最终的答案都是：“这要看法官的心证”。基于《个人资料保护法》的概念，如果能证明企业是无故意无过失，即无需被罚。只是企业要完全证明其无过失责任，以法律观点而论较难以达成，只要发生个人资料外泄，势必还是会被罚，只是做得好，罚得会比较轻。处理得当，可以提升客户对企业的信赖感，亦可提升企业形象，进而创造价值。

个人资料保护的实践只是企业经营过程中的一段插曲，过程中的风险从来不会消失，企业必须在风险中寻找创造价值的能力。

个人信息保护趋势浅谈

梁剑凌　副总监
德勤广州事务所
企业风险管理服务

信息科技和通信网络的持续发展让信息交流和传递变得方便而迅捷，存储设备的发展亦令海量数据的存储和携带变得非常容易。人们在享受信息技术和网络的发展带来的高效和便利的同时，也时时担忧个人信息的丢失和泄漏。同时，随着全球化业务的持续发展，个人信息保护也成为国际业务交流中一项重要指标条件。近年来，频繁发生的个人信息泄漏恶性事件更是将个人信息保护推向了风口浪尖，社会对个人信息保护的关注进入到一个新的高度。

2013年3月，云计算笔记应用Evernote向近5000万用户发出重置密码的通知。Evernote表示，近期遭遇了黑客攻击，导致大量用户名、电子邮件地址和加密密码泄漏。[1] 2013年3月，有消息称支付宝转账信息能够被搜索引擎抓取，致使大量用户个人信息泄漏。[2] 2013年2月，据新闻报道，中国人寿80万份保单信息可在众宜风险管理网任意查询，随后中国人寿发出公告证实消息属实并指出此事故是相关网站升级操作失误所致。[3] 2013年4月，北京警方通报称，近期连续破获两个有组织的侵害公民个人信息的犯罪团伙，抓获92名犯罪嫌疑人，在其中一起案件中，多名保险公司工作人员先后出售20余万条客户信息，被诈骗团伙利用后骗得300余万元。[4]

个人信息泄漏，特别是带有商业价值的个人敏感信息泄漏并遭挪用会给企业造成巨大的经济损失，给相关个人带来精神及名誉伤害。美国FBI于2005年进行的一项调查显示，个人敏感信息泄漏事件的平均损失高达16.7万美元。次年8月，美国司法部的一项研究更是将这一数字提高到150万美元。另外，根据美国市场研究机构Ponemon的一项研究显示，每条泄漏记录的平均损失为86美元，而这些数据的机会成本更是高达每条记录98美元。一家曾发生过数据泄漏事件的美国保险公司更公开表示，其在一次数据泄漏事件中的总损失高达410万美元，平均每条记录损失15美元。

国际著名研究公司Forrester在2007年调查了28家曾发生过数据泄漏事件的公司，其中过半的受访者将数据泄漏后的安全与审计策略的调整成本列为首要损失；而43%的受访者将数据泄漏事件后的客户通知、市场与安全反应以及商业机会损失的成本列为首要损失；同时，39%的受访者称遭受了显著的声誉损失，而25%的受访者称将面临司法处分。[5]

信息泄漏事件的频发及其造成影响的日益严重，人们对自身个人信息的保护意识日益加强，如何有效管理个人信息以及全面保障个人信息免受非法侵害已经成为了国内外热门话题。

有关个人信息保护的原则最重要的是经济合作与发展组织（Organization for Economic Co-operation and Development, OECD）在1980年颁布的《关于保护隐私和个人数据跨国流通指导原则》中有关个人信息保护的8项原则，[6]概括为开放性、个人参与、责任、使用限制、数据质量、收集限制、特殊目的与安全（见表1）。

[1] Evernote遭黑客攻击：要求近5千万用户重置密码.中国信息产业网http://www.cnii.com.cn/internetnews/2013-03/03/content_1101342.htm

[2] 两千支付宝转账信息被谷歌抓取 引发隐私泄露恐慌.新华网新闻http://news.xinhuanet.com/2013-03/29/c_124519198.htm

[3] 中国人寿80万份保单泄露客户数据“裸奔”，腾讯网新闻http://gd.qq.com/a/20130228/000296_3.htm

[4] 新规加大个人信息贩卖处罚：直击非法交易源头.新浪网新闻http://tech.sina.com.cn/t/2013-04-17/10318248454.shtml

[5] Khalid Kark. Calculating The Cost Of A Security Breach. Forrester Research Magazine (April 10, 2007).

[6] 经济合作与发展组织：《关于保护隐私和个人数据跨国流通指导原则》

表1 个人信息保护的8项原则

年份	监管要求
公开原则	必须以方便的方法和人们容易理解的语言向社会公开有关个人信息保护的政策
个人参与原则	信息主体有权知道自身信息的所在位置，有权对自身信息提出质疑，有权对自身信息进行修改、完善、补充和删除
责任原则	个人信息的管理者对个人信息的保管负全责
使用限制原则	对个人信息资料的提供不得超出收集目的，不得随意提供给第三者
数据质量原则	个人信息必须在利用目的范围内保持正确、完整及最新状态
收集限制原则	个人信息的收集必须采取合理合法的手段，必须征得信息主体的同意
目的明确原则	个人信息收集目的要明确化，不能超范围利用
安全保障原则	对个人信息的丢失、不当接触、破坏、利用、修改、公开等风险必须采取合理的安全保护措施

资料来源：经济合作与发展组织。

许多国家以此8项核心原则为依据制定本国的个人信息保护法，并在此基础上不断进行补充和完善。早在1995年，欧盟就出台了涵盖广泛并极具前瞻性的《个人数据保护指令》。1998年6月，美国电子工业协会、美国工商协会和AOL、AT&T、IBM、Bank of America等100多家主要团体和企业成立了在线隐私联盟（Online Privacy Alliances，OPA），发布了《在线隐私指导》。中国台湾地区于1995年出台了《电脑处理个人资料保护法》。次年中国香港出台《个人资料私隐条例》。在中国大陆，2006年大连市推出针对个人信息保护的地区性规定——《大连软件及信息服务业个人信息保护规范》，而改革开放之先锋的深圳也于2010年提出了个人信息保护的立法起草。在2013年中国两会上，政协委员张近东提交了加快制定《互联网个人信息保护法》的提案。

2012年第2季度，上文提及的国际著名研究公司Forrester发表了《Forrsights Security Survey Q2 2012》，其中对当年个人信息数据泄漏事件进行了调研分析。结果显示，信息数据泄漏的源头分为内部组织和外部合作方，其中绝大部分的信息数据泄漏源自企业内部事件，包括公司资产丢失/被盗、内部人员使用不当、针对公司服务器或用户的外部攻击以及内部人员恶意滥用等。

德勤根据多个行业的调查研究和各种类型项目的经验进一步总结出，组织内部泄密风险存在于整个信息处理过程中。信息处理过程围绕着数据信息的生命周期展开，信息生命周期主要分为5个阶段（见图1），分别是信息收集、储存、处理、分发和删除，每个阶段都存在潜在的信息泄漏风险。例如，在信息收集过程中，对外包及第三方活动/服务的监督管理存在缺陷或在个人信息的获取过程中发生资料泄漏等都是个人信息泄漏风险。再者，在信息存储方面同样容易出现泄漏风险。信息的储存介质有纸、胶卷、计算机等，在各种介质中储存的信息都有丢失和被窃取的风险。此外，个人信息的使用如果无法确定使用范围及使用目的，使用信息时就可能引起内外部传播、滥用信息等情况，此时就存在极高的泄漏风险。因此，对于个人信息的管理和保护，我们必须站在信息生命周期的宏观角度进行规划，再深入每个具体过程进行分析和把控。

为了进一步完善有效的控制机制，国内外各机构和组织以个人信息生命周期为模型积极制定一系列指引标准来保护隐私。英国标准协会以戴明环PDCA循环模型（P-Plan; D-Do; C-Check; A-Action）为基础建立了有关个人信息保护指引标准BS10012:2009个人信息管理体系(Personal Information Management System, PIMS)，其中第4.7项规定，在收集信息时，收集最低限度的个人信息而不是过多的个人信息；第4.2和4.13项规定，对存储个人信息的设备需加以维护，保证个人信息存储安全；第4.8项规定，确保个人信息仅用于一个或多个指定的目的，而不能为了其他目的对原信息做进一步的处理；第4.14项规定，当个人信息在内外部传输时，要有足够的保障机制保护个人信息等。总体来

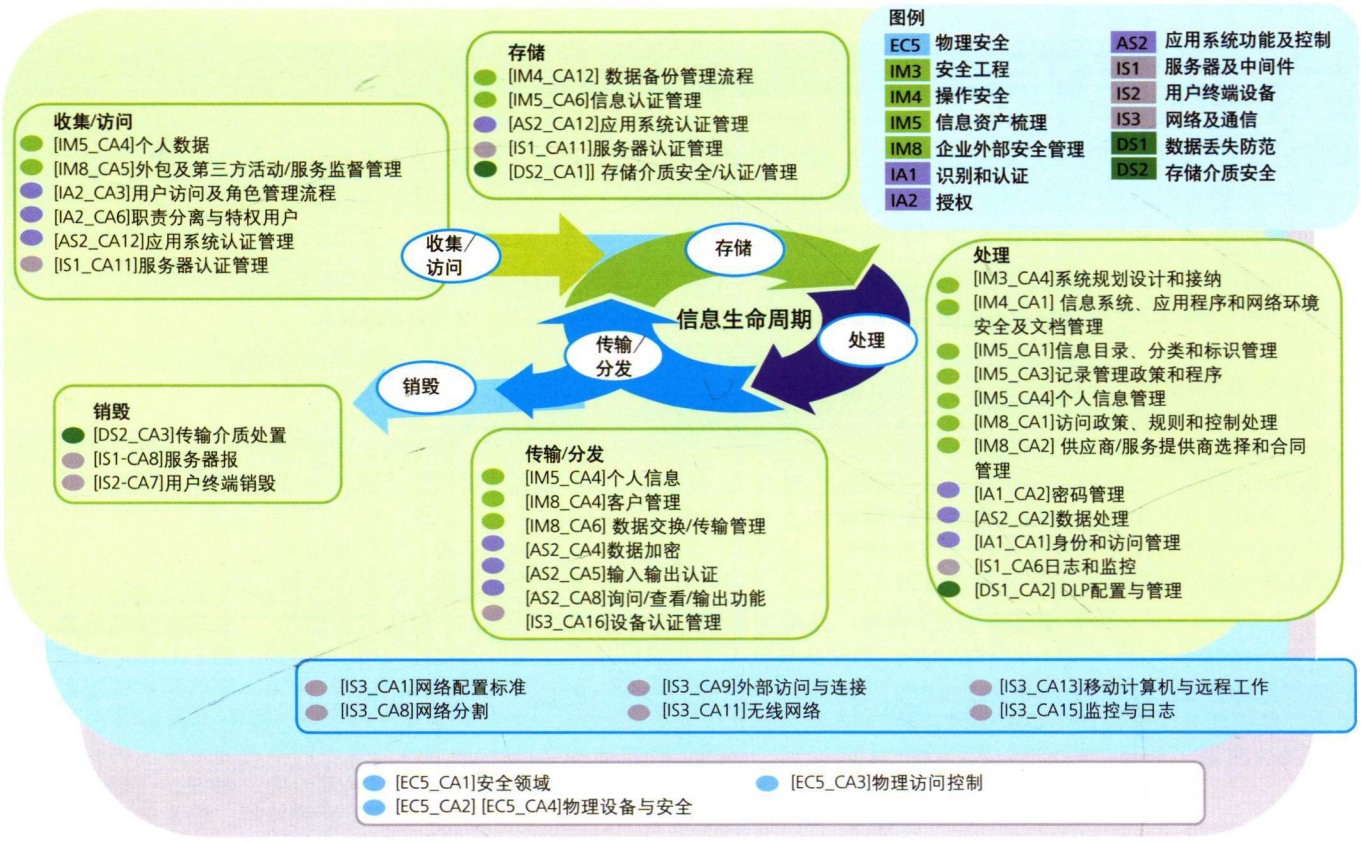


图1 信息生命周期的5个阶段

说，BS10012标准规范几乎覆盖了个人信息生命周期的每一阶段。我国近年来也启动了个人信息保护的相关工作。2012年，国家工信部直属的中国软件测评中心联合30多家单位制定并出台了《信息安全技术、公共及商用服务信息系统个人信息保护指南》，这是我国首个个人信息保护国家标准，于2013年2月1日正式实行。标准对信息系统中的个人信息处理过程的收集、加工、转移、删除阶段进行了规范指引。

个人信息保护的立法正如火如荼地进行着，对于企业而言，建立信息安全机制已迫在眉睫。保护重要的个人信息数据使其免遭泄漏，既可避免声誉受损、客户资源的流失以及严厉的司法处分，又利于保持企业在商业社会的有效竞争力。而一旦这些重要数据外泄，将造成企业重要资产的流失。根据国际隐私权专家协会于2012年针对美国、加拿大、欧洲、亚太平洋等地区的一项调查显示，虽然符合监管机构的法规要求是信息安全投入的最大动因，但降低风险、保护数据紧随其后，成为第二动因。[1] 他山之石，可以攻玉。随着国内企业跨国业务的快速发展以及企业人员国际视野的日益提高，企业对信息安全的关注重点也将逐步转移到风险管理和数据保护等具体层面。目前我国已有众多企业开始采取积极行动，更加主动地关注数据安全，并将数据分析应用于业务的拓展。国内企业开始意识到保护客户个人信息不单单能够满足客户和业务合作伙伴的期望，提高企业的品牌和公信力，提供有竞争力的差异，更能够减少数据存储成本并增加交叉销售和直销的收入。

数据及个人信息安全保护是科技及互联网不断发展的必然产物。企业通过保护数据及个人信息的安全，可以将名誉损失、客户流失以及司法处分等风险降到最低，更可以保护在大数据时代中最重要且核心的资源——数据，并对数据进行有效组织与分析，应用于商业实践，促进企业不断健康地发展。

[1] 国际隐私权专家协会(IAPP). 2012隐私专业人员的角色、职能及薪酬调查.