数据保护官沙龙（DPO Salon）公益出品

英国 Information Commissioner's Office

《数据共享行为守则》(征求意见稿)

中译文

翻译：刘笑岑 田申

审校：曾海泉 蒋艾莉

2019 年 8 月

署名-非商业性使用-禁止演绎 2.5 中国大陆

数据保护官沙龙出品

译者序言

ICO《数据共享行为守则》

——基于源发驱动型的数据安全生态治理

2019 年 7 月 16 日，英国数据保护机构 ICO 就《数据共享行为守则》的修订情况公开向社会征求意见（简称：守则）。守则是基于 GDPR 与英国数据保护法（DPA 2018）而编制的实践指南，旨在提供相关数据合规的指引。截止 8 月初，ICO 已经收到了 101 条反馈意见。

众所周知，数据共享既是数字经济与产业发展的核心环节，更是数据主体权益保护的重大课题。数据融合对经济的促进与对个人隐私的“侵入性”效应同样显著。更为显著的问题是，企业、组织间的数据共享活动外界感知度相对较低，对数据主体权益可能造成的后果归因难且潜伏期长，传统的“检查—执法”监管机制难以发挥有效作用。

在这一背景下，ICO 对守则修订的核心思路以“问责制”为出发点，以保护数据主体权益为核心，通过推动组织间开展数据保护影响评估（DPIA）、订立数据共享协议来落实企业、组织的数据保护主体责任：即企业、组织需要提供 DPIA 评估文档、共享协议等存档资料，表明数据共享活动对数据主体、组织等各方带来或可能带来的收益与损害，并对这些利益进行了认真的权衡，通过法律协议明确数据共享各方的责任与义务，以证明相关数据共享活动符合 GDPR 等数据保护法律的要求。

具体而言，守则对数据共享活动提出了相关具体要求，主要归纳为以下六点：

1.开展数据保护影响评估

1) 作为数据保护法规“可规则性”原则的核心抓手，守则强调即使在法律上并未强制要求组织开展数据保护影响评估的情况下，在数据共享活动中，组织主动遵循 DPIA 程序也是非常必要的，因为数据共享可能会导致对个人的高风险。

2) 开展 DPIA 也是在数据共享前组织所需考虑的第一步，除了 GDPR 中规定的应当开展 DPIA 的四种情形外，对于数据匹配（data matching）、不可见的处理（invisible processing）、在发生数据泄露时可能对个人造成伤

数据保护官公众出品

害的信息处理等情形均需要开展 DPIA。

3) 通过 DPIA 对数据共享活动进行评估，应当综合考虑：

a) 数据共享目的；

b) 共享数据类型；

c) 目的实现是否可以通过不共享数据或共享匿名化数据方式达成；

d) 共享数据对个人信息主体可能造成的侵害；

e) 共享数据对社会和个人潜在的收益与风险；

f) 不共享数据是否会造成损害；

g) 是否有任何法定限制或其他因素对数据共享的限制；

h) 谁会访问这些共享数据；

i) 共享数据是持续性的还是临时性；

j) 共享数据的方式；

k) 共享数据是否已经达成目的，是否需要继续共享数据；

l) 动态重新审查 DPIA，是否有新的变化。

2.订立数据共享协议

1) 订立数据共享协议是证明组织满足 GDPR"可归责性”要求的重要有效途径。因为数据共享协议可以帮助所有各方明确各自的角色，明确规定数据共享的目的，涵盖数据共享各阶段将要处理的事情以及确定数据共享的标准。

2) 在订立数据共享协议中，应当包含下列内容：

a) 数据共享的目的：为何数据共享是必要的、共享数据的具体目的、为个人或者社会带来的好处；

b) 哪些组织会参与数据共享：列明所有参与数据共享的组织，及其 DPO 和其他关键员工的联系方式，在与另一个数据控制者共享数据时，还应当列明自身的责任，并将相关情况告知数据主体；

c) 共享数据的类型：详细说明共享数据的类型，对于某些数据还应当仅允许特定员工访问；

d) 明确数据的共享的合法性基础：是以同意作为披露数据的合法基础，那么协议可以提供一份同意书的模板，并解决有关拒绝或撤回同意的问题；

e) 记录敏感或特殊类别数据：如果共享数据设计特殊或敏感数据，

数据保护官沙龙出品

必须根据 GDPR 或 DPA 的规定记录相应的处理条件。

3) 数据共享协议在满足上述条件外，还应当能够应对数据共享时出现的主要实际问题，以确保参与数据共享的组织满足共享数据最小化原则，确保数据共享准确，使用兼容格式的数据集，共同的保留或删除共享数据规则，共同的技术和组织安全规划，处理公众请求、投诉、询问的程序，协议有效期限以及协议终止的程序。

4) 定期复查数据共享协议，特别是在出现新情况或新的数据共享理由时。

3.贯彻“问责制”原则

1) 根据 GDPR 问责制原则，如组织进行或参与数据共享，须能证明你遵守 GDPR 有关保障数据主体权利的规定。

2) 作为贯彻问责制原则的一部分，在适当的情况下，组织必须制订数据保护政策，并采用“设计及默认方式保护数据”（“data protection by design and default”）的方法，保护数据主体权利。即：采取适当的技术和制度规范来确保数据保护原则的落实，并保护数据主体个人权利。

3) 确保关键文档的留存，例如大型企业、组织需要保留数据处理（共享）活动的记录，并定期对记录进行复盘。

4) DPIA 是问责制的组成部分，签署数据共享协议有助于企业或组织证明符合问责制的要求。

4.确定共享数据的合法性基础

1) GDPR 确定了六项进行数据处理活动的合法性基础，数据共享前应至少确定一个合法性基础。

2) 根据问责原则，企业或组织必须能够显示在开始数据共享之前已经考虑并确定数据共享的合法性基础。

3) GDPR 中的大多数合法基础要求处理是“必要”的。评估合法性基础涉及 DPIA，这要求企业同时考虑必要性和比例性。

5.确保数据共享的公平性和透明度，保障数据主体法定权利

1) 公平和透明是 GDPR 中数据处理原则的核心。

2) 不能以会对他们产生不合理不利影响的方式使用他们的数据。

3) 必须确保共享个人数据是合理和相称的，以及共享个人数据的情况不会出人意料或令人反感，除非有充分的理由。

4) 确保个人知道他们的数据正在如何被共享、处理，哪些组织在共享或获取、访问这些数据，除非适用豁免或例外情形。

5) 共享数据之前，必须以可访问和易于理解的方式告知将如何处理他个人数

数据保护官沙龙出品

据。

6.安全地处理个人数据

安全措施必须与数据处理的性质、范围、背景和目的以及对个人权利和自由构成的风险向适应，并考虑最新技术和实施成本。

通过守则对数据处理活动做出的规范指引可以发现，对数据共享等处理活动的监管措施是通过问责制等制度安排，激发企业、组织的**“源发驱动力”**，通过数据保护影响评估、共享协议等具体措施，将监管的重点由监督审查转向敦促企业、组织“负责任”地开展数据处理与共享活动。

长期以来，数据安全评估、隐私保护合规评审都被认为是增加了企业、组织的负担，而在问责制原则下，这些不仅是法律规定的合规要求，更是在出现可能侵犯数据主体权益的情形出现后，数据保护机构评判责任的重要依据。

数据保护机构会基于风险的执法方法，根据比例原则进行评判：如果企业、组织未开展 DPIA，未能通过协议等方式约束数据共享方的责任，导致数据主体权利受损，则可能面临 2000 万欧元或全球营业额 4%的罚款。因为企业、组织无法证明其切实落实了保护数据主体权益的法律要求。反之，如果在数据共享前认真进行了 DPIA，通过合同、协议等形式严格约束并认真落实，在安全事件、违约情形或第三方因素导致的数据主体权益受损的情况下，则会根据比例原则合理界定其应当承担的责任边界与程度。正如 ICO 在守则中表明的：**“我们将始终按照我们的监管行动政策，以有针对性和比例的方式使用我们的权力。”“我们将一如既往地执法，同时确保商业企业不受繁文缛节的约束，或担心制裁将被不成比例地使用。”**

同样，数据共享组织之间签署协议，本身并不会确保一定符合法律要求，或可以免除法律责任，但是这些是数据保护机构接到有关投诉后去审查和考虑的重要因素。ICO 在守则中明确提到：**“起草和遵守协议本身并不向你提供任何形式的法律保障，使你免于根据数据保护立法或其他法律采取行动。但是，如果 ICO 收到关于你的数据共享的投诉，它将考虑这一点。”**

通过这样的制度设计，企业、组织内部的合规控制流程不再仅仅是付出而无法收回的**“沉没成本”（Sunk Cost）**，而更可以将通过这些程序获得的**“沉默利益”**（笔者将其定义为：通过 DPIA 等风险控制活动而规避的潜在安全风险）显现出来，激发企业、组织以**“负责任”**的方式开展数据处理活动意愿。亦言之，通过制度设计促使企业、组织内部可以从风险控制流程中获得实际的、可见的收益，风险与合规评估由单纯的成本付出活动转变为利益收益活动，形成自发推动并严格落实数据保护措施的**“源发驱动力”**。

近期，我国就《数据安全管理办法》等法律法规公开征求意见，全国信息安全标准化委员会也于 2018 年 7 月公布《个人信息安全影响评估指南》（征求意见

稿)。个人信息安全影响评估对于国内而言仍是刚刚起步，数据监管体系与方式也在探索之中，此次 ICO 发布的《数据共享行为守则》不仅仅是一份合规指引性文件，更是一种构建数据治理生态的方法论。我国当前数据经济蓬勃发展的背景下，这种新型的数据安全治理模式，也许值得行业与监管部门去共同探索。

《数据共享行为守则》发布未满 1 个月，期间笔者还在徒步穿越 130 公里的乌孙古道，评述中的很多观点与思想都是在这条苍凉的古道途中形成并记录的，且囿于个人能力，有诸多不周延之处，仅做抛砖之用。(田申)

数据

数据共享行为守则

（征求意见稿）

数据保护官沙龙出品

目录

数据保护官沙龙出品

数据保护官沙龙出品

前言

信息专员 Elizabeth Denham 的前言将被列入守则的最终版本。

数据保护官沙龙出品

摘要

- 这是根据《2018 年数据保护法》第 121 条制定的法定业务守则。这是一份实用指南，为各组织介绍如何按照数据保护立法共享个人数据。它解释了法律并提供了最佳实践的建议。遵循这一守则和其他 ICO 指南将有助于你：管理风险；达到高标准；澄清你的组织可能对数据共享存在的任何误解；并给予你信心以适当及正确地共享数据。

- 本守则涵盖作为数据控制者的组织之间的个人数据共享情形，也涵盖你以任何方式让第三方访问数据的情形。数据共享可按常规、预定方式或一次性进行。如有需要，数据可在紧急或意外突发情况下共享。

- 在考虑共享数据时，你必须评估你对数据保护立法的整体遵守情况。作为第一步，你应该决定是否需要进行数据保护影响评估（ DPIA ）。我们建议你考虑遵循 DPIA 程序，即使在法律上你没有义务进行数据保护影响评估的情况下。

- 订立数据共享协议是一个好的做法。协议应明确约定数据共享的目的、涵盖数据在每个阶段所须处理的事项、订立标准，并协助各方清楚了解各自的角色。协议有助你证明符合 GDPR 中的可问责性。

- 共享数据时，必须遵循数据保护立法中的关键原则。

- 问责制原则是指你要对遵守 GDPR 或 DPA（视情况而定）负责。你必须能够证明你遵守了这一原则。

- 你必须从一开始就确定至少一个共享数据的合法性基础。

- 你必须始终以公平和透明的方式共享个人数据。当你共享数据时，你必须确保是合理和适当的。你必须确保个人知道他们的数据正在发生什么，除非适用豁免或例外。

- 数据保护法要求你安全地处理个人数据，并采取适当的组织和技术措施。

- 在数据共享安排中，你必须拥有保障数据主体轻松行使其个人权利的政策和程序。

- 为了遵守合法原则，你必须确定你的数据共享的合法性基础，并确保你的数据共享在更广泛的意义上是合法的。

- 大部分的数据共享，以及本守则的大部分内容，都包括在 DPA 第 2 部分的一般处理条文内；在实践中，这是指 GDPR，但"主管当局"为具体执法目的而进行的数据共享，则受制于 DPA 第 3 部分的不同制度，该部分提供了一个独立但互为补充的框架。

- 如果合并或收购或组织结构的其他变化意味着你必须将数据转移给不同的控制者，你必须小心。你必须确保你将数据共享视为尽职调查的一部分。

- 数据库或个人名单的转移是数据共享的一种形式。这可能包括由数据经纪人、营销机

数据保护官沙龙出品

构、信用评级机构、俱乐部和社团以及政党共享。你有责任根据法律规定开展接收和共享数据活动。你必须对数据进行适当的查询和检查，包括数据的来源和获得的任何同意。

- 如果你正在考虑共享儿童的个人数据，你必须谨慎行事。你应该从一开始就考虑到保护他们的必要性。如果数据共享有可能会对儿童的权利和自由造成很大的风险，那么就必须进行 DPIA 。

- 在紧急情况下，你应该按照必要且适当原则共享数据。

- 根据《2017 年数字经济法案》，政府为公共部门的特定目的制定了个人数据共享框架。根据《2017 年数字经济法案》，数据共享必须遵守数据保护立法和符合本守则的业务守则。

- 在决定是否共享个人数据时，除了法律和技术因素外，还应谨记伦理因素。数据信托（Data trusts ）是一个相对较新的概念，可使独立的第三方管理数据。

- ICO 维护公共利益中的信息权利。就数据共享而言，我们关注的重点是帮助你以合规方式开展数据共享。我们将始终按照监管行动政策，以有针对性的和适当的方式行使我们的权力。

数据保护官沙发出品

关于本守则

概要

这是根据 2018 年《数据保护法》第 121 条制定的法定业务守则。

这是一份实用指南，为各组织介绍了如何按照数据保护立法共享个人数据。它解释了法律并提供了良好的实践建议。遵循它和其他 ICO 指南将有助于你：管理风险；达到高标准；澄清你可能存在的任何错误观念；并给予你适当和正确共享数据的信心。

具体内容

- 本守则的地位如何?
- 如果我们不遵守守则会发生什么？
- 进一步阅读"或其他链接资源的状况地位如何？
- 我们应该如何使用这个守则？
- 这个守则主要针对谁？
- 本守则的目的是什么？

本守则的地位如何？

这是根据《2018 年数据保护法》（ DPA ）第 121 条制定的法定业务守则：

「专员必须拟备实务守则，内载─

(a)根据保障数据法例的规定，就共享个人数据提供实务指引；及

(b)专员认为适当的其他指引，以推广共享个人数据的最佳实践。」

本守则根据 DPA 第 125 条于[XXXX]提交议会，并于[XXXX]发布。本守则于[XXXX]生效。

本守则载有关于如何公平、合法地共享数据以及如何履行你的问责义务的实用指导。本守则不会对数据共享设置任何额外障碍，但将帮助你履行 GDPR 和 DPA 规定的法律义务。

它还包含一些可选的良好做法建议，这些建议不具有法律要求的地位，但旨在帮助你采取有效的方法来遵守数据保护。

根据 DPA 第 127 条，专员在考虑你是否已履行与数据共享有关的数据保障责任时，必须考虑本守则。 特别是，专员在考虑 GDPR 和 DPA 所订的公平、合法、透明度和问责性等问

数据保护官沙龙出品

题时，会考虑守则。

本守则也可在法庭诉讼中用作证据，法庭必须在相关情况下考虑其规定。

如果我们不遵守守则会发生什么？

如果你不遵守本守则中的指导，你可能会发现更难以证明你的数据共享是公平、合法和负责任的，并且符合 GDPR 或 DPA 。

如果你违反本守则处理个人数据，导致违反 GDPR 或 DPA ，我们可以对你采取行动。

我们可以使用的工具包括评估通知书、警告、训斥、执行通知书和处罚通知书（行政罚款）。 对于严重违反数据保护原则的行为，我们有权处以最高 2000 万欧元或你全球年营业额的 4%的罚款（以较高者为准）。

如果你没有采纳最佳实践建议，但只要你另想办法遵守法律，则不会有任何惩罚。

"延伸阅读"或其他链接资源的地位如何？

本守则中提及或链接的任何延伸阅读或其他资源都不构成守则的一部分。我们提供链接，以便就具体问题向你提供有用的背景和进一步指导，但根据 DPA ，专员或法院没有法定义务将其考虑在内（除非它是另一个单独的法定实务守则）。

然而，如果我们与其他 ICO 指导相链接，该指导必然会反映专员的意见，并告知我们对解释、遵守和执行的一般做法。

【立法中的相关条款】

See DPA 2018 sections 121, 125 and 127

我们应该如何使用这个守则？

本守则涵盖组织按照 GDPR 以及 DPA 第 2 部所规定的处理体制以及 DPA 第 3 部中的法律执行体制（LE），进行数据共享的行为，。 大多数数据共享很可能是在 GDPR 和 DPA 第 2 部分中规定，但如果条款不同，我们会尽可能澄清这一点。 在这个守则中，有一个单独的章节是关于 LE 处理的，它更详细地描述了差异，但是执行该类型处理的控制者仍然应该阅读整个守则。 本守则不包括 DPA 第 4 部分情报部门制度下的数据共享。

本守则与其他有关数据保护的 ICO 指引及实务守则互相补充。本守则假设你已了解有关数据保护的主要条款及概念的知识。虽然本守则仅作为数据共享的指引，但并不旨在再现其他 ICO 指引，而你有时可能需要参阅 ICO 网站上的指引。这可能是为了概述数据保护法或有关具体概念，义务和权利的更详细指导。守则将突出显示特定实例，以便你参考此类指导。

特别是，在考虑共享数据时，你会发现使用数据保护影响评估（ DPIA ）过程和本守则是有帮助的。 DPIA 的一些或所有问题很可能会在你评估是否适合共享数据以及是否符合法律时对你有所帮助。你可以在守则后面找到关于 DPIA 的更多信息。

数据保护官沙龙出品

【本守则以外的延伸阅读】

ICO's Guide to Data Protection
Guide to Law Enforcement Processing

这个守则主要针对谁？

这个守则主要针对作为数据控制者根据 GDPR 以及 DPA 第 2 部分一般数据处理规定进行数据共享的组织。

控制者的定义见 GDPR 第 4 条。本守则还旨在执法人员在执法处理（LE）制度（第 3 部分 DPA）下的数据共享。第三部分数据共享有一个单独的章节。如果你是这些控制者中的一个，你仍然应该阅读整个代码，它在适当的情况下区分不同的机制。

大部分意见适用于公营、私营及第三部门机构。 有些守则必然侧重于具体部门的问题。然而，守则大部分则适用于所有数据共享，无论其规模和场景如何。

阅读和理解本守则并采纳其实用建议将使你有信心以公平、透明和符合你所共享信息的人的权利和期望的方式收集和共享个人数据。本守则将帮助你确定在共享个人数据之前需要考虑的事项，并明确何时适合你这样做。

【立法中的相关条款】

See GDPR Articles 4(7) and 4(8)
See DPA 2018 section 3(9)

【本守则以外的延伸阅读】

Controllers and processors under the GDPR

这个守则的目的是什么？

这套守则为组织提供实务指引，让它们在遵守保障数据法的情况下，共享个人数据。这套守则解释了有关法律，并推广了良好的做法。

很多使用这套守则的组织，都已在原有的保障数据制度下共享数据。这套守则应该会让你有足够的知识和信心，持续根据 GDPR 和 DPA 共享数据。

本守则：

- 更新并反映了自上次守则发布以来数据保护法的关键变化（特别是来自 GDPR 和 DPA ）；

数据保护官沙龙出品

- 解释了技术的新发展及其对数据保护的影响；
- 供你进行考虑的新领域；
- 帮助你管理数据共享中的风险，如果数据量很大，这些风险会被放大。

关于数据共享的共同担忧

- 本守则还消除了关于数据共享的错误观念和共享障碍。 GDPR 和 DPA 在 2018 年的到来似乎引起了一些组织对数据共享的担忧。然而，数据保护法的许多要求只是将你已经遵循或计划遵循的良好做法置于法律基础之上。

例如：

【误解 1：

数据保护阻止我们共享数据

现实：

数据保护并不阻止数据共享，只要你以一种合理和适度的方式来对待它。本守则帮助你平衡风险和收益，并实现数据共享，如果是：

- 符合公共利益；或者
- 在出于商业原因共享的情况下，符合比例原则。】

【误解 2：

GDPR 为共享数据设置了额外的障碍

现实：

这是错误的。虽然 GDPR 和 DPA 改变了数据保护法的某些方面，但并不妨碍你共享数据。如果你能够在以前的数据保护体制下合法地共享数据，那么很可能你能够在新的数据保护立法下继续这样做，尽管有些差异，我们在本守则中解释了这一点。根据 GDPR ，你必须确定你对共享的决定负责。】

【误解 3：

数据共享几乎没有好处

现实：

数据共享可以为你的组织、个人和整个社会带来好处。如果做得好，它可以帮助政府和商业组织提供现代化、高效的服务，更好地满足人们的需求，使他们的生活更加便利。它还可以识别风险人群，并在他们产生重大不利影响之前解决问题。】

数据保护官沙龙出品

【误解 4：

我们只能在人们同意的情况下共享数据

现实：

不一定。如果你有充分的理由，你通常可以在没有同意的情况下共享（You can usually share without consent if you have a good reason to do so）。但是，在有些情况下，对个人的影响可能会高于你共享数据的利益，在这种情况下，你可能需要征求他们的同意。】

【误解 5：

我们不能在紧急情况下共享数据

现实：

你也许可以这样做。在紧急情况下，你应该做必要的和适当的事情。请参阅守则后面关于这个主题的部分。】

数据共享的好处

本守则还强调了共享个人数据可以给社会、组织和个人带来的好处，无论是作为公民还是消费者。按照法律和良好做法进行的数据共享可以帮助政府和其他组织提供现代、高效的服务，并可以使每个人的生活更加便利。相反，不共享数据可能意味着每个人都无法从这些机会中受益；在某些情况下，错过了帮助有需要的公民的机会，无论是在紧急情况下还是在长期情况下。

你采纳守则的建议的好处可能包括：

- 更好地遵守法律；
- 更好地保护其数据正在被共享的个人；
- 公众对你的信任增加，你可能希望共享他们的数据；
- 更好地了解是否与何时适宜共享个人数据；
- 在你的组织内部对你正在适当和正确地共享数据更有信心；
- 在一次性情况或紧急情况下共享数据的信心增加；
- 在共享数据时声誉风险降低。

【示例 1：

一个地方建立了一个综合护理记录，以便在健康和社会护理人员之间共享患者记录，这就产生了：

数据保护官沙龙出品

- 一个关于患者健康的更全面的情况；
- 整个地区的协调和更安全的护理；
- 围绕患者护理做出更好的决策；
- 患者只需一次讲述自己的病史。】

【示例 2：

医院急诊科和当地的全科医生引入了一个数据共享流程，使医院的临床医生能够 24 小时安全地访问病人的全科医生记录。 这一安排的好处包括：

- 根据既往病史和当前治疗计划，更好地了解患者如何治疗的临床决定；
- 通过识别当前患者药物和过敏情况，提供更安全的护理；
- 减少不必要的紧急入院和重复检查；
- 免除全科医生必须打印这些信息并提供给医院的负担；
- 改善患者体验，降低服务成本，因为临床医生和患者不再需要通过其他方式获得这些信息。】

【示例 3：

一些来自不同组织的健康专业人员参与了为一群老年人提供健康和社会护理的工作，通过交换其中一名服务使用者最近行为变化的信息，他们发现了表明此人可能是虐待受害者的一些证据，他们将这些信息与此人的社会工作者共享，以便进一步调查。】

数据保护官沙龙出品

本守则所涵盖的数据共享

概要

本守则涵盖作为数据控制者的组织之间的个人数据共享情形,也涵盖包括当你以任何方式让第三方访问数据的情形。数据共享可按常规、预定方式进行，也可以一次性进行。如有需要，数据可以在紧急或意外突发情况下共享。

具体内容

- .本守则所包括的数据共享
- .常规数据共享
- .临时或一次性数据共享
- .数据池
- .控制者之间的数据共享
- .与处理者共享数据

本守则所包括的数据共享

立法中并无对数据共享的正式定义，但 DPA 第 121 条将本守则的范围界定为「通过传播、分发或以其他可被他人获得的方式披露个人数据（the disclosure of personal data by transmission, dissemination or otherwise making it available）」。这是指以任何方式将个人数据给予第三方；并包括让第三方在信息技术系统上或通过信息技术系统访问个人数据（This means giving personal data to a third party, by whatever means; and includes when you give a third party access to personal data on or via your IT systems）

就本守则而言，它不包括与员工（employees）或处理者（processors）相关的数据共享。

以下非详尽无遗的清单显示了数据共享可涵盖的内容：

- 各组织之间相互或单向交换数据；
- 某组织为特定研究目的，向另一组织提供其信息技术系统中的个人数据；
- 一个或多个组织提供数据给一个或多个第三方；
- 多个组织汇集信息并相互提供；
- 多个组织汇集信息并向一个或多个第三方提供；
- 为既定目的定期、系统地共享数据；

数据保护专员沙龙出品

- 一次性、特殊或临时共享数据；
- 在紧急或意外突发情况下一次性共享数据。

【数据共享活动实例

- 一所小学向警方或社会服务部门传递了显示受到伤害迹象的儿童的详细信息；
- 警方向一家咨询慈善机构传递了犯罪受害者的信息；
- 一家零售商向一家支付处理公司提供了客户的详细信息；
- 警方和移民局交换了被认为涉及严重犯罪的个人的信息；
- 一家超市向警方提供了客户购买商品的信息；
- 一家地方当局向一家反欺诈机构披露了其员工的个人数据；
- 两家相邻的卫生当局出于预防欺诈的目的共享了其员工的信息；
- 一所学校向一家研究组织提供了其学生的信息；
- 一家多机构网络集团定期交换了个人信息，以达到保护或社会关怀的目的。】

此守则仅适用于共享个人数据。 有些共享不涉及个人数据。 例如，如果一个组织正在共享无法识别任何人的信息（匿名信息；如果你需要更多关于匿名或假名的信息，请参考 ICO 网站 www.ico.org.uk）。 GDPR 、 DPA 和本业务守则均不适用于不构成个人数据的信息共享。

通常认为数据共享可划分为两种主要的不同场景类型：

- 的数据共享，有时称为"系统"数据共享，即相同组织之间为既定目的定期共享相同的数据集；以及
- 基于临时或无法预见或者由于紧急情况或意外突发情况下的特殊目的而例外、一次性地共享数据

不同的方法适用于这两种场景，本守则反映了这一点，本守则的大部分内容集中于常规数据共享。

常规数据共享

这是以常规的、预先计划的方式进行的数据共享。它通常涉及为既定目的在组织之间共享数据，可能是以定期、定期的时间间隔共享相同的数据集。

一种变化情形是，一些集团组织内为了特定的目的，定期共享或汇集他们的数据。

数据保护官沙龙出品

如果你正在进行这种类型的数据共享，你应该事先制定规则并商定程序。

临时或一次性数据共享

有时，组织可能会决定或被要求在任何常规规划或协议未涵盖的情况下共享数据。在这种情况下仍有可能共享数据。我们建议你制定计划，以应对此类突发事件。

有时，你可能不得不在面临现实紧迫性，甚至在紧急情况下，迅速做出数据共享的决定。在这样的情况下，你不应该拖延数据共享；在紧急情况下，你应该做必要和适当的事情。

数据池（Data pooling）

数据池是一种数据共享形式，即组织共同决定汇集他们所掌握的信息，并将其提供给彼此或不同的组织。

负责数据共享的组织将被视为 GDPR 第 26 条下的联合控制者。

控制者之间的数据共享

本业务守则的重点是控制者之间的个人数据共享，即单独或联合控制者决定处理个人数据的目的和方法，如 GDPR 第 4(7)条所定义。

与处理者共享数据

如果控制者要求另一方为 GDPR 的目的代其处理个人数据，则另一方是第 4(8)条所定义的"处理者"。 GDPR 区分了控制者与另一个控制者共享个人数据，以及处理者代表控制者处理个人数据。

GDPR 第 28 条规定了控制者和处理者之间必须有的要求，以保护数据主体的权利。 这些要求包括书面合同和安全担保。在 GDPR 下，处理者必须只根据控制者的书面指令处理个人数据。 根据合同和 GDPR ，处理者有自己的责任和义务。 这种类型的安排不在本守则的范围之内。 更多详情请参考 ICO 网站 www.ico.org.uk 上的指导。

【本守则外的延伸阅读】

Contracts and liabilities between controllers and processors Key definitions: controllers and processors
Guide to the GDPR: controllers and processors

【立法中的相关条款】

See GDPR Articles 4, 26 and 28 and Recitals 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 81 and 82 (external link)
See DPA 2018 section 121 (external link)

数据保护官沙龙出品

数据保护官沙龙出品

决定共享数据

概要

在考虑共享数据时，你必须评估你对数据保护立法的整体遵守情况。作为第一步，你应该决定是否需要进行数据保护影响评估（ DPIA ）。我们建议你考虑遵循 DPIA 程序，即使在法律上你没有义务进行数据保护影响评估的情况下。

具体内容

- 我们需要做什么？
- 我们需要做 DPIA 吗?
- 我们应该考虑哪些因素？
- 在 EEA 之外共享数据

我们需要做什么？

在考虑共享数据时，你必须考虑你整体上是否遵守数据保护法规。作为第一步，你应该决定是否需要进行数据保护影响评估（ DPIA ）。你必须这样做，以证明你遵守 DPIA 条款。即使你没有法律义务进行数据保护，我们建议你考虑遵循 DPIA 程序。

我们需要做 DPIA 吗?

- 你必须为可能会对个人产生高风险的数据共享做 DPIA。这包括一些特殊类型的处理。
- GDPR 给出了需要做 DPIA 的处理实例：
  - 使用创新技术可能对个人权利和自由造成高度风险；
  - 自动决策(包括画像)，产生重大法律效果；
  - 大规模处理特殊类型数据或刑事犯罪数据；以及
  - 对公共空间进行大规模系统性监控。
- 对于任何涉及共享个人数据的其他主要项目，使用 DPIA 也是一个良好的做法。
- 我们认为，要求使用 DPIA 的处理实例可能与数据共享有关，还包括：
  - 数据匹配（data matching）；
  - 可见的处理（ invisible processing DPIA 指南中对此有更详细的说明）；

数据保护官沙龙出品

• 在发生数据泄露时可能对个人造成伤害的信息处理记录，如举报或社会关怀记录。

除了 GDPR 之外，还有一些情况下 DPIA 是强制性的；例如，2017 年数字经济法案中的 pilots

为了帮助你确定是否需要进行 DPIA ，你：

•可以在 ICO 网站上使用我们的筛选检查单；

•应该阅读 ICO 网站 www.ico.org.uk 上关于 DPIA 的指导意见。

如果你有任何涉及披露个人数据的重大项目，或任何例行数据共享的计划，即使没有可能存在高风险的具体指标，你也应该将进行 DPIA 视为良好做法。

如果你已经考虑到共享的性质、范围、场景和目的，并且你确信你所考虑的数据共享类型不太可能导致高风险，那么你可能不需要在法律上进行 DPIA 。尽管如此，你可以使用 DPIA 过程作为一个灵活的、可扩展的工具，以适合你的项目。

我们应该考虑哪些因素？

当你决定是否共享数据时，你应该考虑一些实际和法律因素。

这包括问自己以下问题：

- **共享的目的是什么？**

在决定是否达成共享个人数据的计划（无论是一次性的还是持续的和重复的）时（无论是作为提供者、接收者还是两者），你需要确定共享的目的。你必须有一个或多个明确的目标。这将使你能够确定你需要共享哪些数据以及与谁共享。你必须将此记录在文件中，在数据共享协议（有时也称为信息共享协议）中这样做是一个很好的做法。

- 我们需要共享哪些信息？

你应该只共享实现目的所需的具体个人数据。例如，你可能需要共享某人当前的姓名和地址，但不共享你所掌握的其他信息。

- 我们能在不共享数据或匿名的情况下实现这一目标吗？

如果你能以另一种较少侵入性的方式合理地达到目标，你就不应该处理个人数据。例如，如果你可以通过共享匿名（不适用 GDPR ）的数据来实现这一目标，那么你就应该这样做，因为在这种情况下共享个人数据本身是不合适的。

- 数据共享会给个人带来什么风险？

例如，如果个人可能受到任何形式的伤害，包括身体、情感、经济和社会的伤害。那么个

数据保护官沙龙出品

人是否可以反对？这会破坏个人对保存记录的组织的信任吗？

- 这样共享数据是否正确？

你应该考虑共享数据对社会和个人的潜在好处和风险。在适当的情况下，道德应该成为这些考虑的一部分。请参阅守则后面关于这一问题的章节。数据共享活动的适当性应该是你分析的核心。

- 如果我们不共享数据会发生什么？

你还应该评估不共享数据的可能结果；这本身可能是有害的。

- 我们是否可以共享信息？

检查是否有任何法定限制或其他对数据共享的限制因素。

- 谁要求访问共享的个人信息？

你应采用「需要知道」的原则，即你只应在适当的程度上共享数据：

  - 其他机构只应在有需要时才可查阅你的数据；
  - 而只有这些机构的有关人员才有访问数据的权利。

作为这一工作的一部分，你应该考虑对继续与第三方共享数据可能需要施加的任何必要限制。

- 什么时候该共享？

你必须存档记录这一点，例如，共享是否应该是一个持续的、例行的过程，或者它是否应该只针对特定事件进行，并详细说明这些是什么。

- 我们应该如何共享？

共享数据的过程是什么？这必须包括安全考虑和传输数据的程序，以及所有相关人员对数据的访问。关于这一点的更多内容，请参见守则后面的内容。

- 我们如何检查共享是否达到了目标？

你应该参考你的目标。你试图通过共享这些数据来实现什么？明确这一点将有助于你衡量共享是否成功。然后你可以判断数据共享是否仍然合适，以及保障措施是否仍然与风险相匹配。

- 我们需要重新审查 DPIA 吗？

你必须重新审查所有数据共享安排的风险，就像任何形式的数据处理一样。如果操作发生

数据保护署沙龙出品

重大变化，例如采用新技术，或范围扩大，你应将此视为重新审查任何现有 DPIA （或以前所称的 PIA ）的触发因素，或进行一系列新的评估。

在 EEA 之外共享数据

这些数据是否会转移到欧洲经济区（ EEA ）之外？

我们将在适当时候提供更多关于这方面的指导，同时你应该参考 ICO 网站 www.ico.org.uk 上的指导，以了解最新的情况。

【立法中的相关条款】

See GDPR Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95
See DPA 2018 section 207 (external link)

【本守则延伸阅读】

Data protection impact assessments Detailed guidance on DPIAs
DPIA suggested template
DPIA checklists International transfers Data protection and Brexit

WP29 制定了数据保护影响评估指南，且已被 EDPB 采用。欧洲数据保护委员会（EDPB），取代了 29 条数据保护工作组（WP29），其中包括来自每个欧盟成员国家数据保护当局的代表。它采用了遵守 GDPR 要求的指南。

数据保护官沙龙出品

数据共享协议

概要

订立数据共享协议是一个好的做法。协议需明确数据共享的目的、涵盖每个阶段所须处理数据的事项、订立标准，并协助各方清楚了解各自的角色。协议有助你显示你遵循了 GDPR 中的问责性。

具体内容

- 数据共享协议有什么好处？
- 数据共享协议中应该包括什么？
- 我们应于何时复查数据共享协议安排？

共享和接收数据的各方之间的数据共享协议可以成为你遵守 GDPR 问责原则的主要部分。有时，数据共享协议被称为信息共享协议、数据或信息共享协议或个人信息共享协议。达成协议是很好的做法。

数据共享协议有什么好处？

数据共享协议：

•帮助所有各方明确各自的角色；

•规定数据共享的目的；

•涵盖数据共享各阶段将要处理的事情；

•制定标准。

这有助于你证明你的数据共享是合理的，并证明你已经注意并记录了相关的合规问题。

数据共享协议没有固定格式；它可以采取多种形式，取决于所涉数据共享的规模和复杂性。由于数据共享协议是一套共同规则，对所有参与数据共享的组织具有约束力，你应以易于理解的清晰、简洁的语言起草协议。

起草和遵守协议本身并不向你提供任何形式的法律保障，使你免于根据数据保护立法或其他法律采取行动。但是，如果 ICO 收到关于你的数据共享的投诉，它将考虑这一点。

我数据共享协议中应该包括什么？

为了采用良好做法和遵守数据保护立法， ICO 希望你在数据共享协议中解决一系列问题，包括：

数据保护官沙龙出品

发起数据共享的目的是什么？

你的协议应该解释：

•为什么发起数据共享是必要的；

•你的具体目的；以及

•你希望为个人或更广泛地为社会带来的好处。

你应该用精确的文字记录这一点，以便所有各方都绝对清楚他们可能共享或使用数据的目的。

哪些组织会参与数据共享？

你的协议应明确指出将参与数据共享的所有组织，并应包括其数据保护官（DPO）和其他关键员工的联系方式。它还应包含在数据共享安排中涉及到其他组织的程序，以及处理需要将组织排除在共享之外的情况的程序。

我们是否与另一个控制者共享数据？

如果你与另一个控制者一起作为 GDPR 第 26 条所指的个人数据联合控制者，你需要在“安排”中规定你的责任。这可以通过数据共享协议来实现。根据 GDPR 的透明度要求，你必须将协议的实质内容提供给个人数据主体。我们建议你在提供给他们的隐私信息中这样做。

我们将共享哪些数据项？

你的协议应解释你打算与上述组织共享的数据类型。这可能需要相当详细，因为在某些情况下，只共享文件中关于个人的某些细节是适当的，而不包括其他更敏感的材料。在某些情况下，可能适当地在某些数据项上附加“权限”，以便只允许特定的工作人员，例如接受过适当培训的工作人员，访问这些数据项。

我们共享数据的合法依据是什么？

你需要清楚解释你共享数据的合法依据。如果你是公共机构，你也应该列出你被允许共享数据的法定权力。

如果你是以同意作为披露数据的合法依据，那么你的协议可以提供一份同意书的模板。你还应解决有关拒绝或撤回同意的问题。

是否有任何特殊类别的数据或敏感数据？

如果你共享的数据包含 GDPR 下的特殊类别数据或刑事犯罪数据，或 DPA 第 2 或 3 部分定义的敏感数据，则你必须根据 GDPR 或 DPA 记录相应的处理条件。

关访问权和个人权利如何规定？

数据保护官办公出品

你应该制定符合个人权利的程序。这包括获取信息的权利，以及反对和要求更正和删除的权利。协议必须明确说明，即使你有规定哪些人应执行特定任务的流程，所有控制者仍应保证合规性。

例如，协议应解释当组织收到访问共享数据或其他通知的请求时应做什么。无论是符合数据保护立法、FOIA 或者 EIR。特别是，应确保一名员工（通常是 DPO）或组织全面负责确保个人能够轻松访问所有共享数据。

对于联合控制者，第 26 条要求你在协议中说明哪个控制者负责对行使其数据主体权利的个人作出回应，尽管个人可以选择与任何控制者联系。

你将需要根据具体情况决定访问权限。

对于公共当局，协议还应涉及将某些类型的信息纳入你的 FOIA 发布计划。

我们应该做出什么样的数据治理安排？

你的协议还应处理共享个人数据时可能出现的主要实际问题。这应确保参与共享的所有组织：

- 对于他们可以共享哪些数据集有详细的建议，以防止不相关或过多的信息被披露；
- 确保他们共享的数据是准确的，例如要求定期抽样；
- 使用兼容的数据集，并以同样的方式记录数据。 协议可包括说明应如何记录特定数据项目的例子，例如出生日期；
- 有共同的保留和删除共享数据项目的规则，以及处理不同组织可能有不同法定或专业保留或删除规则的程序；
- 有共同的技术和组织安全安排，包括数据的传输和处理任何违反协议的程序；
- 有处理公众的访问请求、投诉或询问的程序；
- 有评估数据共享的措施和管理该共享措施的协议持续有效的时间期限；
- 有处理数据共享措施终止的程序，包括删除共享数据或将其退回最初提供的组织。

我们应该包括哪些进一步的细节？

如果你的协议有一个附录或附件，可能会有帮助，其中包括：

- 主要立法规定的摘要，例如 DPA 的相关条款，任何为数据共享提供法律依据的立法，以及与任何权威专业指导的链接；
- 寻求个人同意数据共享的示范模板；以及

数据保护官沙龙出品

- 显示如何决定是否共享数据的图表。

你还可以考虑包括数据共享：

•请求表单；

•决策表单。

你可以在本守则的附件 B 中找到这些示例

我们应于何时复查数据共享安排？

你应该定期审查你的数据共享协议，因为在任何时候都可能出现情况的变化或新的数据共享的理由。

你应该定期问自己以下关键问题：

•数据还需要吗？ 这是至关重要的，你必须将任何新的发展因素纳入你对数据共享安排的定期审查，以确保你仍然能够证明共享是合理的。 你可能会发现你已经达到了数据共享的目的，因此没有必要进行进一步的共享。 另一方面，你可能会发现数据共享对你的目标没有任何影响，因此共享不再合理。 如果你不能证明这一点，你就应该停下来。

- 你是否前瞻性地向有关人士传达了你的数据共享安排的任何变化？
- 你的隐私信息和任何数据共享协议是否仍然准确地解释你正在进行的数据共享？
- 你的数据管理程序是否仍然适当并在实践中发挥作用？所有参与信息共享的组织都应检查是否：
- 有必要共享个人数据，或者可以使用匿名信息；
    - 你只共享最少数量的数据，而且最少数量的组织及其工作人员能够访问；
    - 你共享的数据仍然具有适当的质量；
    - 参与共享的所有组织仍然正确地应用保留期限；
    - 参与共享的所有组织已经达到并保持适当的安全水平；
    - 工作人员已经得到适当的培训，并意识到他们对他们能够访问的任何共享数据的责任。
- 你是否仍在为人们提供其在 GDPR 或 DPA 下的所有个人权利？
- 你是否对人们的询问和投诉做出了正确的响应，你是否在分析这些问题以改进你的数据共享安排？

数据保护官沙龙出品

数据保护原则

在共享数据时，你必须遵守数据保护立法的主要原则。不同立法中的原则之间有所差异:

- GDPR 第 5 条
- DPA 第 3 部分第 34-40 关于法律执行

我们在本守则附件 C 中转载了这些原则，请参阅 ICO 网站 www.ico.org.uk 上的详细指导。

【本守则以外的延伸阅读】

Guide to the GDPR: principles
Guide to Law Enforcement processing

数据保护官沙龙出品

问责制

概要

问责原则是指你对遵守 GDPR 或 DPA （视情况而定）负责。你必须能够通过以下方式证明你遵守 GDPR 或 DPA ：

•留存所有数据共享操作的文档；

•实施适当的安全措施；

•记录任何个人数据泄露，并在必要时予以报告；

•对任何可能导致个人利益高风险的数据共享进行数据保护影响评估（ DPIAs ）；

•在适当时任命一名数据保护官员（ DPO ）。

你应该定期审查你的所有问责措施。

具体内容

- 问责原则是什么？
- 设计及默认方式保护的数据保护和设计是什么？
- 我们需要保留哪些文档？
- 数据保护官（DPO）在数据共享规划安排中的作用是什么？

问责原则是什么？

问责制是数据共享的法律要求；它是适用于 GDPR 第 2 部中的一般数据处理和 DPA 第 2 部分以及第 3 部分中的执法处理的原则之一。

问责制原则规定，如你参与数据共享安排，你须负责遵守 GDPR 或 DPA，并须能证明你遵守该规定。作为其中一部分，并在适当的情况下，你必须制订数据保护政策，采用“设计及默认方式保护数据”（ “data protection by design and default”）的方法，以协助你在处理数据时遵守数据保护法及最佳实践。

证明你的遵守情况并证明你的做法是合理的,这是一般义务，因此你应在必要时采取额外措施。数据共享协议将是证明你的问责制的良好做法之一。如果你不能证明你的做法是合理的，那么无论结果如何，你都有可能违反问责制。

问责制原则的重要性如何强调也不为过。要有效地执行问责制，你必须把问责制，从董事会层面，到你的所有雇员，都融入你的组织的文化和业务中。

数据保护官沙龙出品

设计及默认方式保护数据（data protection by design and default）是什么？

“设计及默认方式保护数据”是一项法律义务，要求你采取适当的技术和组织措施以：

•有效实施数据保护原则;

•保护个人权利。

这意味着你必须在整个数据共享过程、计划和活动中严格保护数据。

在关于安全的章节中有更多关于安全的技术措施。其他技术措施包括旨在证明遵守其他义务的技术措施。例如：

•提供同意的证据，包括当时提供的信息的时间戳；以及

•确保正确处理撤销同意或反对，并有效控制细节。

我们需要保留哪些文档？

根据 GDPR 第 30 条，大型组织必须保留其处理活动的记录。 因此，你必须确保记录你进行的任何数据共享，并定期复盘。

了解你拥有的信息，信息的位置以及使用它的方式使你更容易遵守 GDPR 的其他方面，例如确保你持有和共享的信息准确及安全的。

你需要保留足够的文档，以证明你遵守所有原则，义务和权利。 作为其中的一部分，你必须保留同意的记录和任何个人数据泄露的记录。

你必须将数据共享的所有方面以及遵守数据保护法规的其他方面（例如你处理信息的合法性基础和你提供的隐私信息）记录在一起。

数据保护官（DPO）在数据共享安排中的作用是什么？

如果你的组织有 DPO，他应该从一开始就密切参与任何计划，以达成数据共享安排。

当数据共享安排正在进行时，DPO 发挥着重要作用。由于将有许多组织参与，你们每个人都对披露或接受数据承担自己的责任。通常，数据共享安排的目的涉及非常敏感的问题。在每个组织中，DPO 为每个人提供数据治理方面的建议，确保遵守法律，并为面临数据共享决策的员工提供建议。他们也可能是个人行使权利的联络点。

【示例：

警方与地方当局共享了一个关于某一地区帮派的警方情报数据库（帮派数据库）。委员会继续与一些组织不适当地共享它。

不久之后，该地区发生了帮派暴力事件，一些受害者也出现在帮派数据库中。虽然不可能建立与数据泄露的因果关系，但很明显，当此类敏感数据不安全时，可能会有造成痛苦和伤害

数据保护官沙龙出品

的风险。

在这种情况下，很明显，委员会与其他组织共享有大量人员的未经编辑的数据库是不合理和过度的,它应该意识到这样做有明显的风险。

全国都在关注解决帮派犯罪的必要性，人们普遍认为这是公共当局面临的挑战。数据共享在应对这一挑战中发挥着重要作用，但必须依法进行。必须依法、公平、按比例和安全地处理数据。然而，数据保护法并不是数据共享的障碍。

为了帮助防止此类事件的发生，处理敏感数据的组织应制定相应的政策、流程和治理，并对员工进行培训。进行数据保护影响评估（DPIA）是帮助组织确保其遵守法律的一种方法。本数据共享守则也提供了实用的指导。】

【示例：

一个医疗保健组织提供非工作时间的紧急电话服务。 由于可以接到有关客户福利的电话，因此顾问必须能够访问有关组织中的客户的相关个人数据以履行其职责。

一天晚上,一位新顾问接到一个电话，该人自称是警察,并索要其中一名客户的地址。 该组织制定有程序且要求在向第三方共享数据时须予遵守,所有新顾问都必须在任命时接受关于此程序的培训。 因此,顾问知道要遵循的程序来确定他们是否可以共享此信息。】

【立法中的相关条款】

See GDPR Articles 5(2), 25, 28,29,30,31,32,34,35, 38, 39 and Recitals 39, 81-83 (external link) See DPA Part 3

【本守则以外的延伸阅读】

ICO guidance on DPIAs, DPOs, documentation and accountability

数据保护官沙龙出品

共享个人数据的合法性基础

概要

你必须从一开始就确定至少一个共享数据的合法性基础，你必须能够证明你事先考虑过这一点，以满足问责原则。

具体内容

- 什么是共享数据的合法性基础？
- GDPR 下的合法性基础
- .我们如何确定哪一个合法的性基础是适当的？
- 我们如何根据 DPA 第 3 部----执法程序处理，确定哪些法律依据合法性基础是适当的？

什么是共享数据的合法性基础？

你必须从 GDPR 及 DPA 第 3 部分执法处理的若干条文中，找出至少一个共享数据的合法性基础。 这被称为处理的合法性基础。数据共享开始前至少需要确定一个合法性基础。 为了满足 GDPR 和 DPA 第 3 部分中的问责原则，你必须能够显示你在开始数据共享之前已经考虑过这一点。 如果没有至少一个关于处理的合法性基础，你所做的任何数据共享都将违反每一项立法的第一原则。

GDPR 下的合法性基础

关于 GDPR（以及 DPA 第 2 部分）项下的数据分享，第 6 条中包含六个关于处理的合法性基础。它们概括如下。有关详细信息，请参阅 ICO 网站 www.ico.org.uk.

(a)同意：个人已明确同意你为特定目的共享他们的个人数据.

(b)合同：共享是履行你与个人签订的合同所必要，或因为他们要求你在订立合同前采取特定步骤.

(c)法律义务：共享是你遵守法律(合同义务除外)所必要.

(d)重要利益：共享是保护某人的生命所必要.

(e)公共任务：共享是你为了履行公共利益任务或官方职能所必要，任务或职能在法律上有明确的依据.

(f)合法利益：共享是为了你的合法利益或第三方的合法利益所必要，除非有充分的理由保护个人数据应凌驾于合法利益之上，特别是当个人是儿童的时候。 如果你是处理数据以执行公务的公共机构，你不能以合法利益作为你的合法性基础。

数据保护官沙龙出品

我们如何确定哪一个合法性基础是适当的？

你应该仔细考虑数据共享计划的所有背景细节。相关因素包括：

- 数据的性质；
- 你共享数据的目的；
- 共享的背景；以及
- 你与个人的关系。

GDPR 中的大多数合法性基础要求处理是“必要”的，以达到特定目的。此评估涉及 DPIA 过程，这要求你同时考虑必要性和比例性。问问自己：

- 你的计划是否有助于实现你的目标？
- 是否有其他合理的方法来实现相同的结果？

"必要"意味着数据共享必须不仅仅是有用的，或者说是标准的实践。 它必须是一种有针对性和相称的方法，客观上是实现你所说的具体目标所必需的。 如果你可以通过一些其他较少侵扰的手段，或者通过共享较少的信息来合理地达到目的，那么你就没有数据共享的合法性基础，你就不应该这样做。

在你开始处理任何个人数据之前，你应该决定适用哪些合法性基础。 从一开始就选择适当的合法性基础是很重要的。 在没有充分理由的情况下，你不应该在以后转换到另一个合法性基础上。 • 特别是，你通常不能从“同意”切换到其他的合法性基础。

通知中告诉个人你共享他们数据的合法性基础，以及你必须提供的其他细节。• 关于隐私信息的详细信息请参见守则后面内容。

关于如何确定哪些合法性基础适合你所考虑的数据共享的更多信息，请参阅 ICO 网站上的指导意见，网址为 www.ico.org.uk。

如将合法利益作为合法性基础，我们需要做些什么？

如果你将合法利益作为向第三方披露数据的合法性基础，你必须开展第三方测试，即合法利益评估（LIA）。这种测试会考虑与 DPIA 相同的一些问题，考虑数据共享的必要性以及个人权利。ICO 网站上可看到更多关于此方面的信息 www.ico.org.uk

在特殊类别数据和刑事犯罪数据方面我们需要做些什么？

一些数据共享安排涉及特殊类别数据。如果你在 GDPR 下共享特殊类别数据，则必须确定共享的合法性基础以及这样做的附加条件。第 9（1）条禁止处理特殊类别数据，但第 9 条第（2）款列出了允许在某些情况下处理的条件。第 9 条第（2）款所列的某些条件受 DPA 附表 1 第 1 部分的条件限制。概言之，这些涉及以下领域：

- 就业；
- 社会保障和社会保护；
- 卫生和社会护理；
- 公共卫生；以及
- 档案、研究和统计。

如果你计划共享的数据涉及刑事定罪、刑事犯罪或相关的安全措施，根据 GDPR 第 10 条，你必须确定一般处理的合法性基础，并拥有"官方权力"或满足 DPA 附表 1 下处理这些数据的单独条件。

我们如何根据 DPA 第 3 部----执法处理，确定哪些合法性基础是适当的？

对于根据执法规定进行的数据共享，只有在"以法律为依据并在其范围内"以及满足以下两种情况之一才是合法的：

•个人同意为此目的进行数据共享；或者

•数据共享对于主管当局为此目的执行任务是必要的。

我们需要如何处理 DPA 第 3 部分下的敏感处理？

在执法处理方面，“敏感处理”一词类似于特殊类别的数据。如果你想共享属于该项下的任何数据，你必须满足 DPA 第 3 部第 35 条所列两种情况中的一种要求：

第一种情况：

- 为有关执法目的而共享该数据的数据主体的具体同意；以及
- 在进行共享时，你必须拥有第 42 节所定义的“适当的政策文件”。

第二种情况：

- 为了执法目的，处理是绝对必要的；
- 处理至少符合附表 B 的一个条件；以及
- 在进行共享时，你有一份合适的政策文件。

【立法中的相关条款】

See GDPR Articles 6(1)(c), 6(1)(e), 6(1)(f), 6(3), 9(2), 13(1)(c), 14(1)(c),

数据保护官沙龙出品

and Recitals 39, 41, 45, 47-49, 50, 51 See DPA 2018 sections 7, 8, 10, 11, 35, 42 and Schedules 1 (paras 6 and 7) and 8.

【本守则以外的延伸阅读】

Lawful basis for processing
Lawful basis interactive guidance tool Legitimate interests
Legitimate interests assessment Guide to
law enforcement processing

数据保护官沙龙出品

数据共享的公平性和透明度

概要

你必须始终以公平和透明的方式共享个人数据。

- 你必须公平对待个人，不能以会对他们产生不合理不利影响的方式使用他们的数据。
- 当你共享个人数据时，你必须确保共享是合理和适当的。 你还必须确保共享的方式不会出人意料或令人反感，除非有充分的理由。
- 你必须确保个人知道他们的数据正在发生什么。 他们必须知道哪些组织正在共享他们的个人数据，哪些组织可以访问这些信息，除非适用豁免或例外。
- 在共享数据之前，你必须以可访问和易于理解的方式告诉个人你提议如何处理他们的个人数据。

具体内容

- 我们在共享数据时如何遵守公平原则？
- 我们在共享数据时如何遵守公平原则？
- 我们需要根据 GDPR 提供什么隐私信息？

公平和透明是 GDPR 中数据处理原则的核心。你必须以公平和透明的方式处理个人数据。

根据 DPA 第 3 部分的执法规定，公平也是原则的重要组成部分。DPA 第 44 条就第 3 部分的处理规定了透明度。

我们在共享数据时如何遵守公平原则？

这一原则适用于 GDPR 下的一般处理和 DPA 第 3 部分下的处理。

- 你必须公平对待个人，不能以会对他们产生不合理不利影响的方式使用他们的数据。
- 当你共享个人数据时，你必须确保共享是合理和适当的。
- 你还必须确保共享的方式不会出人意料或令人反感，除非有充分的理由。 除非你是出于法律义务而共享，或者共享对于执法来说是必要的；尽管有任何此类顾虑，数据共享仍将进行。
- 无论共享的类型如何，你都必须遵守公平原则：无论你是在例行基础上共享数据，还是进行单次一次性披露。

数据保护官沙龙出品

- 除了证明你有数据共享的合法性基础外，你还必须满足数据共享的公平性要求。 如果你处理的任何方面是不公平的，你将违反公平原则-即使你可以证明你有合法性基础进行处理。

- 你必须公平对待被你共享数据的数据主体。 如果你在数据共享安排中公平对待大多数个人，但不公平对待一个人，这仍然是违反这一原则的。

最后，有时数据处理可能会对个人产生负面影响，但这并不一定是不公平的，关键是这种不利是否合理。

我们如何评估我们是否公平地共享信息？

一些需要考虑的问题：

- 你打算做的事情是否公平？你对数据共享的规划过程-包括作为 DPIA 一部分的步骤（无论你是否需要完成 DPIA ）将有助于你评估这一点。

- 你是否应该共享个人数据？考虑这一点，以及考虑如何共享个人数据。

- 你是如何获得这些数据的？例如，在你获得这些个人数据时，是否有人受到欺骗或误导？如果是这样，那么将这些数据用于共享就不太可能是公平的。

- 数据共享如何影响其一般数据主体的利益？

在共享数据时，我们如何遵守透明度要求？

个人必须知道他们的数据正在发生什么。GDPR 及 DPA 第 3 部分第 44 节所要求的透明原则，是指你必须确保个人知道哪些组织正在共享他们的个人数据，哪些组织可以访问这些数据，除非有豁免或例外情况。

在数据共享前，你必须以可访问及易于理解的方式，告知个人你建议如何处理他们的个人数据。你必须使用适合你的用户的清晰及浅显的语言。

我们需要根据 GDPR 提供什么隐私信息？

当你从个人收集个人数据时，根据 GDPR 第 13 条，你必须向他们提供隐私信息，其中列出你打算如何收集和使用他们的数据，以及谁将参与其中，包括接收者或接收者的类别。这样做是你遵守透明度义务的一部分，在适当的情况下，也是履行公平原则的一部分。

当你从第三方收集个人数据时，根据第 14 条，你必须在合理的期限内并最迟在一个月内向个人提供隐私信息。 在数据共享场景中，这可能是控制者共享和接收数据。 当你首次向另一个接收者披露数据时，你必须在“最迟”期限内向个人提供信息。

向个人提供隐私信息的方法不同。你可以使用一种或多种技术提供隐私信息，但你必须：

- 包括某些特定内容；

数据保护官沙龙出品

- 如果你改变了数据共享的目的或开始新的数据共享，请保持更新并主动发布新信息；并且
- 将信息直接提供给个人。

有关更多详细信息，请参阅 ICO 网站 www.ico.o 上的指南

【立法中的相关条款】

See GDPR Articles 5(1)(a), 13, 14 and Recitals 39, 58, 60-62 (external link)
See DPA 2018 Part 3 section 44 (external link)

【本守则以外的延伸阅读】

ICO guidance on the right to be informed.

ICO guidance on the first principle

数据保护官沙龙出品

安全

概要

数据保护法要求你安全地处理个人数据，并采取适当的组织和技术措施。安全措施必须与数据处理的性质、范围、背景和目的以及对个人权利和自由造成的风险相适应。在确定哪些措施适合你的情况时，你还必须考虑到最新技术和实施成本。

具体内容

- 数据保护法对安全有何规定？
- 共享数据时的安全注意事项是什么？
- 在共享数据后，我们是否仍要负责？

数据保护法对安全有何规定？

数据保护法要求你安全地处理个人数据，并采取适当的组织和技术措施。安全措施必须与处理的性质、范围、背景和目的以及对个人权利和自由造成的风险相适应。

本章适用于 GDPR 和 DPA 第 3 部分下的处理。这些是指以不同方式处理数据的安全措施：

- GDPR 的安全原则要求你使用“适当的安全性”…“使用适当的技术或组织措施（“完整性和保密性”），并在第 32 条中进一步说明。
- 对于根据 DPA 第 3 部分进行的执法处理，你必须使用“适当的技术或组织措施”，以确保个人数据的适当安全。

在确定哪些措施适合你的情况时，你还必须考虑到最新技术和实施成本。

共享数据时的安全注意事项是什么？

对于你与其他组织共享信息或他们与你共享信息，你应考虑以下措施：

- 审查你从其他组织收到的个人数据。确保你知道它的来源，以及它的使用是否附带任何条件；
- 查看与其他组织共享的个人数据。确保你知道谁访问它，他们会用它做什么；
- 在共享特殊类别或敏感数据时，确保提供适当的高安全级别；
- 确定组织内哪些人应该能够访问与你共享的数据。采用“需要知道”原则，避免在只有少数员工需要数据来执行工作时让所有员工访问数据；

数据保护官沙龙出品

- 考虑个人数据泄露对个人的影响；以及

- 考虑个人数据泄露可能对你的组织造成的影响，包括成本、声誉损失或缺乏客户或客户的信任。例如，当个人向你提供了他们的数据，你与另一个组织共享数据，而该接收组织未能保护这些数据时，这种情况尤其严重。

你应该致力于在整个组织中建立一种合规文化和良好实践，以帮助你确保安全地共享数据。这必须贯穿董事会层面、所有员工和承包商等各层面。例如：

- 参与数据共享的所有员工必须了解保护个人数据的重要性；以及

- 你应该检查在与你共享数据的组织中是否同样适用。

在共享数据之前，你应该进行信息风险分析并记录你的结论。作为评估的一部分，你应该记住你共享的信息的性质。例如，它是特殊类别还是敏感数据？你应该定期测试和评估你的安全条款。

这必须包括正在共享的数据的实际传输，以及以后处理数据的方式。你应该考虑为保护数据而需要采取的措施。

但是，你不能忘记安全的所有其他方面，包括物理和技术方面。你需要确保在你自己的办公场地以及与你共享数据的组织（在适当情况下）了解并定期审查你的物理和技术安全措施。细节很重要，包括谁可以访问数据，以及对所有硬件和软件的访问控制是什么。记住，在发生停电或火灾等事件时，要考虑建筑物和办公室的安全以及恢复能力。

当你通过多种方式（如电话、传真、邮寄、电子邮件、在线或面对面）共享信息时，你还应该清楚地了解需要遵循的安全步骤。

在共享数据后，我们是否仍要负责？

与你共享数据的组织对数据承担自己的法律责任，包括数据的安全性。但是，你仍应采取合理措施，确保你共享的数据将继续受到接收方组织的充分安全保护：

- 确保收件人了解信息的性质和敏感性；

- 采取合理措施确保安全措施到位，特别是确保你已将一套商定的安全标准纳入你的数据共享协议（如果你有）；以及

- 如果你和接收组织的安全标准不同、IT 系统和程序不同、保护性标记系统不同等，你应在共享个人数据之前解决存在的任何问题。

对任何数据共享操作进行 DPIA 是考虑这些问题和实施适当缓解措施的有效手段。

你还应该注意，在某些情况下，在数据共享时需要执行 DPIA。请参阅本规范“决定共享数据”一章中有关 DPIA 的部分。

数据保护官办公室出品

【立法中的相关条款】

See GDPR Articles 5(1)(f), 32, 35, and Recitals 39, 83 (external link)

See DPA sections 40 and 91

【延伸阅读-ICO 指南】

更多信息请阅读我们关于 GDPR 的安全指南。

ICO 与 NCSC 紧密工作制定了安全成果，你可以用来判断什么是适当的。安全成果也可在你考虑任何数据共享安排中有所帮助。】

数据保护官沙龙出品

个人权利

概要

在数据共享中，必须具有允许数据主体轻松行使其个人权利的政策和程序。你应该为他们提供一个单一的联系点，并与其他组织有明确的政策和程序。你必须通知其他组织有关删除、更正或限制处理的请求，除非这样做不可能或不合理的。

如果你的数据共享涉及自动化决策，则还有其他要求。

在执法处理中，个人权利的立场略有不同。

具体内容：

- 个人权利对数据共享有何影响？
- 你如何允许个人在数据共享场景中行使其信息权限？
- 删除、更正或限制处理请求对数据共享安排有何影响？
- 我们如何处理个人关于共享数据的投诉和疑问？
- 如果数据共享涉及自动化决策，我们需要做什么？
- 根据第 22 条的规定，对于完全自动化的处理，我们需要做什么？
- DPA 第 3 部分：执法处理提供了哪些个人权利？

个人权利对数据共享有何影响？

在数据共享安排中，必须具有允许数据主体行使其个人权利的政策和程序。

根据 GDPR 和 DPA 第 3 部分，个人可享有的权利在某些方面有所不同。

GDPR 赋予个人对其个人数据的特定权利。对于根据 DPA 第 2 部分进行的一般数据处理，总结如下：

- 访问有关个人数据的权利（主体访问权）；
- 有权了解如何以及为什么使用他们的数据，并且你必须向他们提供隐私信息；
- 更正、删除或限制其数据的权利；
- 反对权；
- 数据的可移植性权利；以及

数据保护官沙龙出品

- 不受仅基于自动化处理的决定约束的权利。

本章并不试图复制现有的 ICO 关于个人权利的指导，而是关注权利如何影响数据共享。更多详细信息，请参阅 ICO 网站 www.ico.org.uk 上的指南。

你如何允许个人在数据共享场景中行使其信息权限？

- 你必须有允许个人轻松行使权利的政策和程序。
- 如果你是联合控制者，应在你和你的其他联合控制者须根据 GDPR 第 26 条订立的透明安排中明确规定
- 你必须在向个人发布的隐私信息中提供如何行使这些权利的详细信息。
- 你必须使得权利的行使尽可能简单。请注意，虽然你的 DPO 负责作为第一联系人，但个人可以联系你组织的任何部分。
- 当多个组织共享数据时，个人可能很难决定应该联系哪个组织。你应该在收集他们的数据时向他们提供的隐私信息以及根据第 26 条作出的任何透明安排中明确说明数据主体应该联系哪个组织。
- 在数据共享安排中，为个人提供单一联系点（a single point of contact）是一种良好的做法，这允许他们对共享的数据行使权利，而无需向多个组织提出多个请求。但是，允许他们选择对任何他们希望的控制者行使他们的权利。

对删除、更正或限制处理请求对数据共享安排有何影响？

根据 GDPR 第 16、17 和 18 条，个人有权要求删除、更正其数据或限制其数据处理。与其他个人权利一样，如果你对如何处理这些请求有明确的政策和程序，你将使自己和数据共享中的其他组织的活动更轻松。

根据 GDPR 第 19 条，如果你与其他组织共享信息，则必须告知他们个人数据的更正、删除或限制途径，除非这不可能或涉及不合理。如果被要求，你还必须告知个人这些组织的情况。

我们如何处理个人关于共享数据的投诉和疑问？

有时，个人可能会对共享其个人数据产生疑问或投诉，特别是当他们认为数据错误或共享对他们有不利影响时。

处理这些疑问和投诉的方式对个人和组织都有影响。这并不总是简单地提供响应的情况。当你查看数据共享安排时，你收到的评论可能是非常宝贵的资源。

最好的做法是：

- 有快速有效处理任何投诉和疑问的程序；

- 提供单一的联系人（a single point of contact）；
- 分析你收到的评论，以便更清楚地了解公众对你进行的数据共享的态度；
- 在回答个人的具体问题时，利用这个机会向个人提供超出隐私信息的更多的关于你的数据共享的信息；
- 如果你在告知他人你的数据共享时收到的答复包含大量的反对意见、负面评论或其他关切表述，请使用此信息帮助你审查相关的数据共享；
- 考虑你收到的评论是否建议你减少共享的数据量，或者与更少的组织共享数据；
- 特别注意提出的问题，并决定在面对公众反对时是否可以继续共享。例如，你可能决定继续进行，因为你负有共享数据的法律义务；以及
- 如果你正在进行大规模数据共享操作，请考虑建立焦点小组，以探讨个人的顾虑。

如果数据共享涉及自动化决策，我们需要做什么？

如果你的数据共享安排涉及任何自动化决策，你必须在数据保护政策（ data protection policy）中记录该自动化决策的具体合法性依据。

为了让个人行使他们的权利，你必须：

- 向他们提供有关自动化流程及其风险的信息；
- 如果你间接获得了他们的个人数据，请向他们发送一个指向你的隐私声明的链接；
- 解释他们如何访问你用于创建其用户画像的信息的详细信息；
- 告诉那些向你提供个人数据的人，他们如何反对用户画像，包括出于营销目的用户画像；以及
- 告知他们，并制定相关程序，告知他们有权访问用户画像使用的个人数据，以便他们为了更加准确而审查和进行编辑。

此外，为了保护任何弱势群体（包括儿童），你必须在数据共享中检查用户画像/自动化决策系统。你必须始终确保只收集所需的最少数量的数据，并为你创建的用户画像制定明确的保留策略。

根据第 22 条的规定，对于完全自动化的处理，我们需要做什么？

如果你的数据共享安排有一个对个人具有法律或类似重大影响的单独的自动化决策程序，则 GDPR 第 22 条赋予个人额外的保护权利。例如，自动化用户画像，取决于对个人的影响。你必须执行 DPIA，其中你需要根据 GDPR 第 35（3）（a）条评估你提议的数据共享（包括基于自动化处理的系统化和广泛的性用户画像）将“对自然人产生法律影响，或对自然人产生类似影响”。

数据保护官沙龙出品

只有在以下情况下，才能执行此类自动化决策：

- 与个人签订或履行合同所必需的；
- 经法律授权（在本守则中，我们正在研究英国的具体法律规定，例如用于反欺诈或逃税）；或
- 基于个人的明确同意。

你必须确定数据共享、的任何因素是否属于第 22 条的范围。如果有，你必须：

- 向个人提供有关自动处理的信息；
- 为他们介绍简单的方法，要求人为干预或挑战决策；以及
- 定期检查以确保系统按预期工作。

DPA 第 3 部分：执法处理提供了哪些个人权利？

- 知情权；
- 访问权；
- 纠正权；
- 删除或限制处理的权利；以及
- 不受自动决策影响的权利。

GDPR 下的某些权利，如反对权和数据可移植权，不存在于法案的第 3 部分。在某些情况下，还可以合法地适用豁免和限制，以防止个人行使权利。在 ICO 网站 www.ico.org.uk 上有更多关于这方面的指导。

数据保护官沙龙出品

【示例：

提供儿童保育服务的第三部门组织可能持有地方当局和 NHS 共享的信息。第 26 条透明度规划应规定一个明确的程序，即无论哪个组织收到个人数据要求，都应率先提供数据，并在必要时通知其他方。

该规划还应规定如何处理行使其他个人权利的程序。

这些程序也应在隐私信息中提供，并应包含在任何数据共享协议中。】

【立法中的相关条款】

See GDPR Articles 16-19 and 22
Part 3 of the DPA

【本守则以外的延伸阅读—ICO 指导】

ICO guidance on the rights of data subjects
Individual rights under the Law Enforcement Processing provisions

数据保护官沙龙出品

其他法律要求

概要

除了确定数据共享的合法基础外，你还必须确保你的数据共享在更一般意义上是合法的，以便遵守合法性原则。

对于公共部门机构，这包括确定你是否具有共享数据的合法权限。

大多数私营和第三部门组织不需要确定共享数据的特定权力。只要不违反数据保护立法或任何其他法律，他们就具有共享信息的一般能力。如果你是一个私营部门组织，你应该检查你的章程文件、法律协议或任何其他法律或监管要求，以确保没有任何限制会阻止你在特定环境中共享个人数据。

具体内容

- 我们有权共享数据吗？
- 公共部门的法律权力是什么？
- 私营和第三部门组织组织的法律权力是什么？
- 人权法的影响是什么？
- 你是否检查过数据共享是否有任何法律禁止？

本守则考虑了数据保护立法的数据共享要求。本章将介绍一些其他要求。它讨论了对你的法律限制、数据保护立法之外的限制，以及你共享数据所需的法律权限。

在共享任何个人数据之前，你必须考虑这样做的所有法律含义。除了确定数据共享的合法基础外，你还必须确保你的数据共享在更一般意义上是合法的，以便遵守合法性原则。对于公共部门机构，这包括确定你是否具有共享数据的合法权限。

你不能把合法性原则和法定权力混为一谈。不过，有一个关联——如果你没有合法的权限共享数据，那么你将违反合法性原则。

我们有权共享数据吗？

如果你希望通过一次性披露或作为常规数据共享规划的一部分与其他组织共享信息，则需要考虑：

- 例如，根据你的宪法，你是否具有共享信息的一般法律权力。这可能与公共部门组织更为相关；以及
- 你是哪种类型的组织，因为你的法律地位也会影响你共享信息的能力，特别是取决于

数据保护官沙龙出品

你是属于公共部门、私营部门还是第三部门。

公共部门的法律权力是什么？

在决定你是否可以进行任何数据共享活动时，你应该确定与你相关的立法。即使它并没有明确提及数据共享——而且通常不会这样做——它很可能会让你更清楚地了解自己的法律地位。

大多数公共部门组织的权力完全来自法规——要么来自设立它们的议会法案，要么来自监管它们活动的其他立法。例外情况是由一位政府部长领导的政府部门（他们有普通法权利共享信息）。

相关立法可能会根据你的目的、你必须做的事情以及为实现这些目的而行使的权力来界定你的职能。因此，你应该确定所讨论的数据共享在你所能做的事情的范围内（如果有的话）将适合哪些地方。从广义上讲，有三种方式可以做到这一点：

- **明确法定义务**

  有时，公共机构将在法律上有义务与指定组织共享特定信息。只有在非常特殊的情况下才会出现这种情况。

- **明确的法定权力**

  有时候，公共机构会有明确的权力来共享信息。明示权力通常被设计为允许出于某些目的披露信息。明确的法定义务和共享信息的权力通常被称为“网关”。例如，根据 2017 年《数字经济法》（DEA），存在特定的网关。根据 DEA，有一个框架为特定公共当局之间的特定目的的数据共享提供了一个法律网关，以实现公共利益。有关详细信息，请参阅本守则的其他部分。

- **隐含的法定权力**

  通常，监管公共机构活动的立法在数据共享问题上是沉默的。在这种情况下，可以依靠一种隐含的权力来共享立法明文规定的信息。这是因为可以采取明确的法定权力来授权组织做其他事情，而这些事情是明确允许的。公共当局可能依赖 GDPR 第 6（3）条中的公共任务合法性基础。这要求权力由法律规定，但这不需要是一个明确的法律规定。只要数据具有足够的可预见性和透明性，就可以依靠这种权力力来共享数据。

无论你共享信息的权力来源是什么，你必须检查该权力是否涵盖相关的特定披露或数据共享规划。如果没有，你不得共享信息；除非在特定情况下，即披露中存在高于一切的公共利益。

私营和第三部门组织的法律权力是什么？

适用于私营和第三部门组织的法律框架与适用于公共部门组织的法律框架不同。大多数私营和第三部门组织不需要确定共享数据的特定权力。只要不违反数据保护立法或任何其他法

律，他们就具有共享信息的一般能力。如果你是一个私营部门组织，你应该检查你的章程文件、法律协议或任何其他法律或监管要求，以确保没有任何限制会阻止你在特定环境中共享个人数据。复杂或大规模数据处理的大型组织应考虑寻求法律建议。

私营和第三部门组织应注意有关处理个人数据的任何行业特定法规或指导，因为这可能会影响你共享信息的能力。

人权法的影响是什么？

公共当局在履行其职能时必须遵守《1998 年人权法》。HRA 也适用于私营部门的组织，只要它们执行公共性质的职能。

在《人权法》适用的情况下，各组织不得以与《欧洲人权公约》（《公约》）规定的权利不相容的方式行事。《公约》第 8 条赋予每个人尊重其私人和家庭生活、家庭和通信的权利，特别涉及个人数据的共享。

如果你仅以符合数据保护立法的方式披露或共享个人数据，则共享或披露该信息也可能符合 HRA。

如果你对人权问题有任何顾虑（第 8 条的数据保护要素除外），你应寻求专家建议，了解你提议的披露或数据共享规划。

你是否检查过数据共享是否有任何法律禁止？

你共享信息的能力可能受到数据保护立法之外的一些法律限制。可能还有其他的考虑因素，例如的具体法定禁止共享、版权限制或可能影响您共享个人数据能力的信任义务

保密义务可以通过信息的内容或在预期保密的情况下收集的信息（如医疗或银行信息）明确规定或暗示。如果你是一个计划执行复杂或大规模数据处理的大型组织，则应考虑就数据共享计划寻求法律建议。

在某些私营部门的情况下，除了数据保护立法外，还存在披露个人数据的法律限制。

【立法中的相关条款】

欧洲人权公约：第 8 条

【本守则以外的延伸阅读】

Lawful basis for processing
Guide to Law Enforcement Processing

数据保护官沙龙出品

执法处理：DPA 第 3 部分

概要

大多数数据共享，以及由此产生的大部分规则，都包含在 DPA 第 2 部分的一般处理规定中；实际上，这意味着指的是 GDPR。然而，“主管当局”为特定执法目的共享的数据受到 DPA 第 3 部分关于执法处理的不同制度的约束，该制度提供了一个单独但补充的框架。作为主管当局，你很可能也会出于 DPA 第 2 部分的一般目的处理个人数据，例如与人力资源相关的事务。在这种情况下，你应该遵循第 2 部分/GDPR 数据共享的一般指南。

具体内容

- 什么是主管当局？
- 什么是执法目的？
- 我们是主管当局：我们如何共享数据？
- 我们如何与主管当局共享数据？
- 在第 3 部分中的数据共享场景中，我们如何允许个人行使其信息权利限？
- 我们如何遵守第 3 部分中的问责制要求？

出于执法目的，为什么需要数据共享通常是有说服力的原因的。我们知道，在这种情况下，组织有时会对数据共享犹豫不决。然而，我们强调，当有必要保护公众、支持正在进行的社区警务活动或紧急情况时，数据保护并不能阻止适当的数据共享。遵守法律规定并遵循本守则中规定的良好做法将有助于你以符合要求和适当的的方式共享数据。

【示例：

主管当局提出的信息请求必须在其执法目的范围内合理，并应向组织明确说明请求的必要性。

例如，警方可能会要求社会工作者将案件档案转交给警方，其中包含青少年的详细信息。

如果请求明显过多，或者必要性或紧迫性明显不合理，社会工作者可能不愿意主动向警方披露信息。警方应尽可能在不影响调查的情况下提供清晰的请求信息。

大多数数据共享，以及由此产生的大部分规则，都包含在 DPA 第 2 部分的一般处理规定中；实际上，这意味着指的是 GDPR。然而，主管当局为特定执法目的而共享的数据受 DPA 第 3 部分规定的不同制度的约束，该制度提供了一个单独但补充的框架。】

什么是主管当局？

主管当局是指：

数据保护官沙龙出品

- DPA 附表 7 中规定的人员；或
- 任何其他人员，如果且在一定程度上，他们有法定职能行使公共权力或公共权力，以实现执法目的（DPA 2018 第 30（1）（b）节）。

你需要检查你是否在 DPA 的附表 7 中被列为主管当局。该名单包括大多数政府部门、警察局长、HMRC 专员、假释委员会和 HM 土地登记处。

如果你没有在附表 7 中列出，如果你有权为执法目的处理个人数据，则你仍可能是主管当局。例如，在起诉环境犯罪时起诉贸易标准犯罪的地方当局或环境署。

执法目的是什么？

该术语在 DPA 第 31 节中定义为：

【引述

预防、调查、侦查或起诉刑事犯罪或执行刑事处罚的目的，包括防范和预防对公共安全的威胁”。】

执法必须是处理的主要目的。

即使你是主管当局，你也很有可能为 DPA 第 2 部分的一般目的处理个人数据，而不是出于执法目的。人力资源相关事务就是一个例子。在这种情况下，你应该遵循本守则其他地方包含的通用数据共享指南。

我们是主管当局：我们如何共享数据？

如果你是主管当局，并且共享是出于执法目的，那么第 3 部分可能会提供一个允许你共享数据的框架。

这在某些方面不同于第 2 部分和 GDPR 中的规定。这些差异包括合法性基础，主要是因为你处理数据的目的不同。

特别是，第 3 部分只有六项原则，第 3 部分中描述为“敏感”的数据处理受到额外保障，如 DPA 附表 8 中的条件。

我们如何与主管当局共享数据？

如果你是一个不属于主管当局第 3 部分定义的组织，那么出于执法目的，你仍然可以与主管当局（如符合 GDPR 的警察）共享数据。但是，你必须有合法的共享基础，并且你可能还需要一个条件来披露 DPA 附表 1 中的数据。

主管当局提出的信息请求在其执法目的范围内必须是合理的，并且应向你清楚地说明请求的必要性。

在这种情况下，如有必要，你还可以依赖 DPA 附表 2 第 2（1）段中的“犯罪和税收”豁

数据保护官沙龙出品

免，不受某些 GDPR 规定的约束。这包括透明度义务和大多数个人权利，如果这些规定的适用可能损害预防或侦查犯罪。

如果你不是主管当局，并且正在披露与刑事犯罪和定罪（包括指控）有关的数据，你必须遵守《全球发展政策》第 10 条。实际上，这意味着：

- 你需要再次满足 DPA 2018 附表 1 中的相关条件。在这种情况下，最有可能出现的情况是附表 1 第 10 段：为防止或发现非法行为所必需的披露；以及

- 如果满足公共利益要求是一个问题，附表 1 第 36 段规定了一个让步条件，允许披露刑事犯罪数据，前提是披露是防止或侦查非法行为所必需的；而要求独个人的同意将损害这些目的。

如果你共享的数据包括特殊类别数据（例如关于种族、族裔、宗教或生物特征数据的信息），在大多数情况下，GDPR 第 9 条下的条件需要与 DPA 附表 1 中的关联条件一起适用（最有可能是第 9（2）（g）条）。根据 DPA 第 10 段中的附表 1），你必须能够证明，出于重大公共利益的原因，数据共享是必要的。

DPA 通常要求组织具有“适当的政策文件”，以涵盖在这种情况下的处理。然而，向主管当局披露数据的组织不需要有政策文件来涵盖该披露。

【示例：

一位店主使用闭路电视，并经常拍下该店顾客的录像。警方要求提供一些闭路电视录像的副本，以推进正在进行的刑事调查。警方告诉店主为什么要这样做（一些主管部门可能会使用标准的表格）。

店主根据 GDPR 规定处理数据。假设店主有合法的处理依据，她可以依靠附表 1 第 10 段来处理闭路电视数据，并向警方提供录像副本，以帮助调查。

接收警方（主管当局）根据 DPA 2018 第 3 部分处理信息。这有助于它履行其法定职能。】

在第 3 部分中的数据共享场景中，我们如何允许个人行使其信息权利？

在执法处理中，个人权利的可用性存在差异。GDPR 下的某些个人权利，如反对权和数据可移植权，在 DPA 的第 3 部分中不存在。在某些情况下，可以合法适用豁免和限制，以防止个人在可能损害执法目的的情况下行使权利。

有关详细信息，请参阅 ICO 执法处理指南，网址：www.ico.org.uk。

我们如何遵守第 3 部分中的问责制要求？

DPA 的第 3 部分要求你作为控制者证明你遵守这些原则。你是有责任的。

你必须制定适当的技术和组织措施，以确保并证明你遵守。这可能包括策略和过程，包括设计及默认方式数据保护。

【示例：

在本守则关于问责制一章中，有一个例子，是关于一个委员会不适当地从一个有关帮派的警察情报数据库中披露未经记录的信息。

警方在这类例子中自己使用帮派数据库还需要解决数据保留、安全、过度数据收集和共享等关键问题，以使帮派计划合法化。警察和公共部门组织（如地方议会）之间的数据共享来打击帮派文化的目的是为了追求有效公共利益。

一种公平的数据共享方法，其目的是透明的，并对数据保护法规定的义务负责；将获得我们最直接受影响的社区的信任，从而增强社区警务人员与他们接触的能力。】

你还必须维护数据处理活动的相关文档。有关更多详细信息，请参阅 ICO 执法处理指南。

我们在下面列出了第 3 部分数据共享文档的特殊要求。

类别

为执法目的共享数据时，如果相关且尽可能，你必须明确区分不同类别的个人数据。你必须区分以下人员：

- 涉嫌或即将实施刑事犯罪（嫌疑人）；
- 被判刑事犯罪；
- 是或被怀疑是刑事犯罪受害者的个人（受害者）；或
- 作为证人或能够提供犯罪信息的个人（证人）。

处理活动的内部记录

在第 3 部分中，你必须保存你所从事的所有数据处理活动的详细记录。这是一项法律义务。你的记录必须包括你期望的详细信息，例如：

- 处理的目的（这显然包括任何数据共享规划）；
- 与你共享个人数据的组织类别；
- DPO 的名称；以及
- 你的安全措施。

记录

以下可能适用于执行数据共享的许多主管当局。如果你的组织为数据处理操作任何 IT 数据库，那么在第 3 部分中，你必须保存特定处理操作的日志，例如收集、更改、删除和披露

数据保护官沙龙出品

（包括传输）。有关更多详细信息，请参阅 ICO 执法处理指南。

【立法中的相关条款】

See GDPR Articles 6, 9, 10 and Recitals 40, 41, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56 (external link)

See DPA 2018 sections 10, 11(2), 15, 30(1)(b), 31 and schedule 1 (paragraphs 10 and 36), 2 (paragraph 2) and 7 (external link)

【本守则以外的延伸阅读】

Guide to Law Enforcement Processing
Guide to data protection

数据保护官沙龙出品

合并和收购后共享数据时的尽职调查

概要

如果合并、收购或组织结构的其他变化意味着你必须将数据传输到其他或额外的控制者，则必须小心。你必须确保将数据共享视为你进行的尽职调查的一部分，包括确定最初获取数据的目的以及共享数据的合法性基础。你必须遵守这些原则，并记录你的数据共享。考虑何时以及如何通知个人他们的数据发生了什么。你还必须确保健全的管理、责任和安全。

本章与私营部门特别相关。它强调了一些情况，例如合并和收购，或者组织结构的其他变化，在这些情况下，你需要优先考虑好数据共享实践。

具体内容

- 数据共享如何应用于合并和收购？
- 在合并、重组或其他控制权变更之后，我们如何管理共享数据？

数据共享如何应用于合并和收购？

• 当合并或收购或组织结构的其他变化意味着你必须将数据传输到不同的组织时，数据共享考虑可能成为优先考虑事项。例如，作为收购的一部分，数据可以作为资产出售给不同的法人。如果由于更改而导致数据的控制者发生更改，或者数据正在与其他控制者共享，则必须小心。无论你是共享控制者还是接收人是控制者，都是如此。我们将从组织与不同的控制者共享数据的角度来看待这一点：

- 确保你将数据共享视为尽职调查的一部分；
- 遵循本守则中的数据共享指南；
- 确定要传输的数据；
- 确定最初获取数据的目的；
- 建立共享数据的合法基础；
- 确保你遵守数据处理原则，尤其是从合法性、公平性和透明度开始；
- 记录数据共享；
- 在共享涉及不同系统的数据之前寻求技术建议：存在可能导致数据丢失、损坏或降级的潜在安全风险；以及
- 考虑何时以及如何告知个人发生的事情。

数据保护官沙龙出品

- 根据 GDPR，你需要让个人数据主体了解与他们的数据处理相关的某些变化，他们可能有权反对。请参见 ICO 网站 www.ico.org.uk 上的个人权利指南。

同样的考虑也适用于接收数据的控制者。

在合并、重组或其他控制权变更之后，我们如何管理共享数据？

在实践层面上，在这种类型的更改之后，很难立即管理共享数据，特别是当你使用不同的数据库，或者你试图集成不同的系统时。在这一时期，考虑 GDPR 的治理和问责要求尤为重要。你必须：

- 检查数据记录是否准确和最新；
- 确保记录你对数据所做的一切；
- 遵守所有记录的一致保留政策；以及
- 确保适当的安全措施到位。

【立法中的相关条款】

See GDPR Articles 5, 6, 7 and 21 and Recitals 39, 40, 42, 43, 50, 69, 70

【本守则以外的延伸阅读】

Guidance on individual rights under the GDPR

数据保护官沙龙出品

在数据库和列表中共享个人数据

概要

有关个人信息的数据库或列表的转移，无论是出于利益或其他考虑，无论获利与否，都是一种数据共享形式。这可能包括数据经纪人、营销机构、信用评级机构、俱乐部和社团以及政党的共享。

你有责任使自己对提供给你的数据的完整性得到保障。你有责任确保接收的数据遵守法律，并且你必须对任何有关该数据的投诉作出回应。你应进行适当的查询和检查，包括：

- 确认数据来源；
- 确定其获得的合法性基础；
- 检查个人在移交数据时被告知的内容；
- 核实最初收集数据的方式和时间细节；
- 检查同意记录（如相关）；
- 审查收集数据时提供的隐私信息副本；
- 根据 GDPR-ie 隐私信息第 14 条，检查向个人提供了哪些信息，当从数据主体以外的来源获得数据时，必须提供这些信息；
- 检查数据是否准确和最新；以及
- 确保你收到的数据不过度或与你的需求无关。

具体内容

- 数据共享如何应用于数据库和列表的获取或传输？
- 我们必须做些什么来确保我们收到的数据库或列表是按照法律共享的？
- 我们还需要做什么？
- 数据共享如何与直销互动？
- 数据共享如何与政治竞选互动？

数据共享如何应用于数据库和列表的获取或传输？

有关个人信息的数据库或列表的转移，无论是购买或其他考虑，还是为了利润，都是一种

数据保护官沙龙出品

数据共享形式。本章讨论的数据共享不是由组织变化引起的。

参与此类数据共享的组织包括：

- 数据经纪人；
- 信用评级机构；
- 营销机构；
- 特许经营；
- 独立于总部运营的业务的各个部分；
- 俱乐部和社团；
- 慈善机构；以及
- 政党。

数据保护立法允许你这样做，只要你遵守法律。你还将发现遵循本守则中规定的良好实践是有益的。共享方和接收控制方进行的尽职调查对合规性至关重要。

我们将从接收数据库或列表的组织的角度来看待这一点。共享数据的组织应该遵循类似的过程。

我们必须做些什么来确保我们收到的数据库或列表是按照法律共享的？

你有责任确保提供给你的数据的符合完整性要求。你有责任确保获取的数据符合法律规定，并且你必须对任何有关该数据的投诉作出回应。你应进行适当的查询和检查，包括以下内容：

- 确认数据来源；
- 确定其获得的合法性基础；
- 检查个人在移交数据时被告知的内容；
- 核实最初收集数据的方式和时间细节；
- 检查同意记录（如相关）；
- 审查收集数据时提供的隐私信息副本；
- 根据 GDPR-ie 隐私信息第 14 条，检查向个人提供了哪些说明，当从数据主体以外的来源获得数据时，必须提供这些说明；

数据保护官沙龙出品

- 检查数据是否准确和最新；以及
- 确保你收到的数据不过度或与你的需求无关。
- 你应该考虑与提供数据的组织签订书面合同。

我们还需要做什么？

根据 GDPR 第 14 条，“在获得个人数据后的合理期限内，但最迟在一个月内……”，你必须向共享数据涉及的个人提供隐私相关的信息。

数据共享如何与直接营销互动？

如果这种数据共享形式与你的数据共享规划有关，你应该阅读 ICO 关于直接营销的详细指南。我们将发布最新的直接营销实践准则；你应参考 ICO 网站 www.ico.org.uk。

数据共享如何与政治竞选互动？

政党、全民公决活动家和候选人利用选民的信息来帮助更有效地针对他们的竞选材料；他们可以：

- 从数据经纪人等组织购买列表和数据库；以及
- 利用第三方发送竞选材料。

这涉及到数据共享；与选民的沟通，例如通过社交媒体平台和针对性的政治信息，可能就相当于直接营销。

你应该执行本章前面描述的检查，以满足你对所提供数据的完整性的要求。

如果你使用第三方组织代表你使用数据库发送竞选材料，那么你将与该外部组织共享数据。在检查和监控第三方所做的工作时，你应该勤勉尽责。你作为该数据的控制者负责遵守法律。你应在 www.ico.org.uk 网站上阅读并遵守有关政治竞选和直接营销法律的 ICO 指南。

【立法中的相关条款】

See GDPR Articles 13 and 14

【本守则以外的延伸阅读—ICO 指导】

请参阅 ICO 网站上的直销守则及指引 www.ico.org.uk

请参阅即将在 ICO 网站上发布的新政治竞选指南 http://www.ico.org.uk/www.ico.org.uk

See the Guide to Privacy and Electronic Communications Regulations (PECR)

数据保护官沙龙出品

数据保护官沙龙出品

数据共享与儿童

概要

如果你正在考虑共享儿童的个人数据，你必须谨慎行事。你必须考虑到儿童的最大利益。你应该从一开始就考虑保护他们的必要性。

你应该将其构建到数据共享规划中的系统和流程中。高水平的隐私应该是你的默认设置。

我们建议你进行 DPIA 以评估共享此数据所涉及的风险。与第三方共享儿童数据会使他们面临风险。如果数据共享是一种可能对儿童权利和自由造成高风险的类型，那么 DPIA 是强制性的。

具体内容

- 在共享儿童数据时，我们需要注意什么？

在共享儿童数据时，我们需要注意什么？

- 你需要考虑孩子的最大利益。这一概念来自《联合国儿童权利公约》（UNRC），该公约声明，“在涉及儿童的所有行动中，无论是由公共或私人社会福利机构、法院、行政当局或立法机构采取的，对儿童的核心利益应是首要考虑因素。“本质上，儿童的最大利益是对该儿童个人最有利的。

- 你必须平衡儿童的最大利益与他人的权利。例如，一个组织的商业利益不太可能超过儿童的隐私权。

- 考虑到儿童的最大利益应构成你遵守合法、公平和透明原则的一部分。

- 公平性和遵守数据保护原则应该是你对儿童个人数据进行共享的核心。共享儿童的数据是否公平？共享的目的是什么？

- 儿童对收集和处理数据所涉风险的了解程度低于成年人，因此你有责任评估风险并采取适当措施。在设计数据共享规划时，请考虑儿童的意见。

- 你提供的隐私信息必须清晰，并以适合其年龄的语言呈现。

- 你应该对计划与之共享数据的组织进行尽职调查。你应该考虑与你共享数据的组织计划如何处理这些数据。如果你可以合理地预见数据将以对儿童有害的方式使用，或者其他方面不公平，那么你不应该共享。

- 你应确保任何与数据共享相关的默认设置都指定了共享的目的以及与谁共享数据。允许一般或无限制共享的设置将不符合要求。

- 你不应该共享个人数据，除非你有充分的理由这样做，并且同时考虑到儿童的最佳利益。一个明显的令人信服的理由的例子是用于保护目的的数据共享。而出售儿童的个

数据保护官办公室出品

人数据以进行商业再利用不太可能成为数据共享的一个令人信服的理由。

- 同意不是唯一的合法性基础。其他合法性基础可能更合适。

  如果你的合法性基础是基于同意，你必须考虑孩子的自己的同意，以及是否自由给予该同意（例如，在权力不平衡的情况下）。

  如果你依赖于合法履行合同所必需的合法性基础，你还应该考虑孩子的能力。

- 如果你（或数据共享计划中的其他数据控制者）是在线服务的提供者，那么你还需要遵守适用于年龄的设计规范。

在 ICO 网站 www.ico.org.uk 上有关于上述所有内容的更多信息

【立法中的相关条款】

See GDPR Articles 6(1), 8, 12(1) and Recitals 38, 58, 65, 71, 75

【本守则以外的延伸阅读】

Guide to data protection: children Children and the GDPR

United Nations Convention on the Rights of the Child

数据保护官沙龙出品

紧急或意外突发情况下的数据共享

概要

在紧急情况下，您应该继续并根据需要和比例共享数据。如果您可能参与应对紧急情况，通过考虑您所持有的数据类型以及您可能需要提前分享的数据，尽可能提前做好计划是有帮助的。

更多内容

- 紧急情况下我们该怎么办？
- 在紧急情况下，我们如何提前计划数据共享？

本守则中的大部分指导思想都设想你将在常规基础上执行数据共享，并且你有机会和时间提前仔细计划。然而，情况并非总是如此。

意外突发情况下我们该怎么办？

紧急或意外突发情况可能会出现，你可能没有预想，而必须当场处理。在意外突发情况下，你应该继续进行，并根据需要适当的共享数据。

近年来的悲剧，如格伦菲尔大厦火灾，以及伦敦和曼彻斯特的重大恐怖袭击，都表明了联合公共服务的必要性，在这些服务中，数据共享可以对公共安全产生真正的影响。在这种情况下，不共享数据比共享数据更有害。你应该考虑不共享数据所涉及的风险。

在紧急情况下，我们如何提前计划数据共享？

在紧急情况下，你必须迅速做出决定。通常，提前计划会有所帮助。针对各种情况制定应急服务计划，同样，你应该提前为组织制定计划。在紧急或意外突发情况下，如果没有足够的时间来详细考虑问题，就很难对是否共享信息做出正确的判断。

同样，组织和机构在计划和恢复阶段都不愿共享信息也是有原因的，因为在计划和恢复阶段，共享信息的需求可能并不那么迫切。

关键是，DPA 不会阻止组织在适当的情况下共享个人数据。在这种情况下，考虑不共享数据所涉及的风险尤其重要。

在可能的情况下，如果你可能参与应对紧急情况，你应该考虑到可能需要提前共享的数据类型。作为其中的一部分，考虑任何现有的 DPIA 都会很有用。所有这些都有助于你确定所保存的相关数据，并有助于防止紧急情况下的任何延迟。

所有类型的组织都可能面临紧急但可预见的情况，因此，你应该对你所持有的个人数据，是否共享以及如何共享这些信息有一定的程序。

数据保护官沙龙出品

【示例：

警方、消防部门和地方议会齐聚一堂，计划在洪水、重大火灾或恐怖事件等意外突发情况下，识别和协助所在地区的弱势群体。作为这一过程的一部分，他们决定各自持有何种类型的个人数据，并达成一份数据共享协议，规定他们将共享哪些数据，以及在紧急情况下如何共享这些数据。

他们定期审查这个计划。】

数据保护官沙龙出品

公共部门数据共享：数字经济法案守则

概要

根据《2017 年数字经济法》（DEA），政府为公共部门特定部分的特定目的设计了一个个人数据共享框架。其目的是在确保隐私的同时，通过更好地使用数据来改善公共服务，并确保公共部门共享数据的方式的清晰性和一致性。DEA 准则要求与本数据共享准则保持一致，为严格定义的 DEA 数据共享权力的按比例行使提供指导，并符合数据保护立法。

根据《2017 年数字经济法》（DEA）：DEA 框架，政府引入了一个框架，用于在公共部门的特定部分为特定目的共享个人数据。（注意，DEA 框架不同于 DPA 第 191 节中的政府数据处理框架）。

其目的是确保公共部门共享个人数据的方式的清晰和一致性，通过更好地使用数据改善公共服务，同时确保数据隐私。政府还明确表示，只有在有明确的公共利益的情况下才应该共享数据。

DEA 的第 5 部分着重于数字政府，提供允许特定公共当局彼此共享个人数据的网关，以改进公共服务的提供。DEA 权限下的数据共享目标和目的是严格定义的。

这些组织仍然必须遵守数据保护立法。

DEA 第 5 部分明确：

- 声明 DEA 权力下的所有信息处理必须符合数据保护立法；以及
- 禁止在违反数据保护立法的情况下披露信息。

注意，虽然 DEA 早于 GDPR，但其起草目的是为了与 GDPR 规定保持一致。

根据 DEA 第 5 部分共享信息的权力由法定行为守则（DEA 守则）补充，本守则必须与信息专员的“不时更改或替换的”数据共享行为守则一致。这些守则必须遵循数据保护原则，确保 DEA 权力下的个人数据共享是适当的的。

例如，公共当局有一个 DEA 守则，用于共享有关以下公共服务交付方面的个人数据信息：

- 实现特定的公共服务交付目标；
- 帮助生活在燃料贫困和水资源贫困中的人们；以及
- 管理针对公共部门的债务和欺诈。

DEA 中还规定了促进统计局和统计局共享数据的规定，以允许统计数据的产生、民事登记官员披露信息以及为研究目的共享数据。

数据保护官沙龙出品

DEA 守则包含关于你可以共享哪些数据以及用于何种目的的指南。其中包括确保公民数据隐私受到保护的保障措施。公共当局必须制定一项数据共享协议，在 DEA 守则中称之为“信息共享协议”。

根据 DEA 第 5 部分权力披露信息的任何人还必须“考虑”信息专员发布的其他实践守则“只要适用于相关信息”：

- 识别和降低信息披露建议的隐私风险；以及
- 向个人提供关于使用从个人收集的信息的说明。

【立法中的相关条款】

Digital Economy Act 2017

【本守则以外的延伸阅读】

Digital Economy Act Part 5 Codes of practice

数据保护官沙龙出品

数据伦理与数据信托

概要

在决定是否共享个人数据时，除了考虑法律和技术因素外，还应考虑道德因素。数据信托是一个相对较新的概念：一个允许独立第三方管理数据的法律体系。已经进行了一些试点项目来证明它们在数据共享中的用途。

具体内容

- 什么是数据信托？
- 共享这些数据是否合乎伦理？
- 数据信托领域发生了什么？
- 数据伦理领域发生了什么？

什么是数据信托？

无论是在英国还是在国际上，“数据信托”的概念都引起了极大的兴趣。数据信托有多种定义。开放数据研究所（ODI）将其定义为“提供独立第三方数据管理的法律体系”（ “a legal structure that provides independent third-party stewardship of data”）。从本质上讲，它们是一种能够通过新技术（如人工智能）访问数据，同时保护其他利益和保持信任的新的模式，并遵循“设计隐私”方法。它们有可能用于数据共享。

数据信托领域发生了什么？

2019 年，英国政府宣布，ODI 将与其他人合作开展试点项目，以研究数据信托如何在保持信托的同时增加对数据的访问。还宣布，在适当时候，ODI 将就未来使用数据信托提出建议。

ICO 将在未来发布更多关于数据信托的信息；请访问 ICO 网站 www.ico.org.uk。

共享这些数据是否合乎伦理？

在决定是否进行数据共享规划时，你应该从道德角度考虑共享将如何影响个人的信息权利。问问自己是不是：

- 以特定方式共享数据的权利；
- 负责组织的行动；
- 合理证明；以及
- 受到明确和强有力的保障？

数据保护官沙龙出品

数据保护原则基于尊重个人基本权利。这反映在数据保护立法对处理个人数据时公平、透明和问责制的要求中。从广义上讲，伦理原则是对比例和公平性的考虑的一部分，是对数据保护原则的补充。除了考虑数据共享的合法性和技术要求之外，你还应该考虑它们。

我们还应该考虑什么？

你还应考虑：

- 权力的不平衡。组织和个人，特别是弱势个人之间的权力严重失衡。作为一个组织，你不仅要对更广泛的社会的需要负责，还要对个人的需要负责；以及
- 数据共享将对个人在社会排斥等问题以及平等和基本人权问题上的信息权产生影响。
- 这些可能正是你打算在数据共享计划中帮助解决的问题，因此你需要仔细考虑，因为你可能需要实现微妙的平衡。

数据伦理领域发生了什么？

英国政府对数据伦理感兴趣。

2017 年，它宣布成立数据伦理与创新中心（CDEI），对公共部门和私营部门使用数据和数据技术以及人工智能进行调查和咨询。

2018 年，它发布了一个数据伦理框架，规定了公共部门应如何使用数据的明确标准，旨在建立对公共部门数据使用的信心。

2015 年，英国统计局（UKSA）成立了国家统计师的数据伦理咨询委员会，向国家统计师提供独立和透明的建议，即收集、获取、使用和共享数据用于研究和统计目的是合乎道德的，并且为了公众利益。

UKSA 还开发了一个自我评估工具包，为研究人员在研究过程中如何评估和减轻道德风险提供指导和支持。

【本守则以外的延伸阅读】

Open Data Institute website ODI
article on data trusts
Government data ethics framework
Centre for Data Ethics and Innovation website
The National Statistician's Data Ethics Advisory Committee

数据保护官沙龙出品

执行守则

概要

• ICO 维护公众利益的信息权。在数据共享的背景下，我们的重点是帮助你以兼容的方式进行数据共享。

• 在适当情况下，我们有各种权力对违反 GDPR 或 DPA 的行为采取行动。这包括发出警告、谴责、立即停止命令和罚款的权力。我们将始终按照我们的监管行动政策，以有针对性和比例的方式使用我们的权力。

具体内容

ICO 的作用是什么？

信息专员是英国独立的数据保护监督机构。

我们的使命是维护数字时代公众的信息权利。我们的数据保护愿景是提高公众对处理个人数据的组织的信心。我们提供建议和指导，推广良好做法，监控和调查违规报告，监控合规性，进行审计和咨询访问，考虑投诉，并在适当情况下采取执法行动。我们的执法权力载于 DPA 第 6 部分。

我们还推出了沙盒（Sandbox）等计划，以帮助使用个人数据开发创新产品和服务的组织。

如果本守则的规定与其他监管机构重叠，我们将与他们合作，确保一致和协调的响应。

ICO 将如何监控合规性？

我们将在工作中使用本守则，通过我们的审计计划和其他活动评估控制者的合规性。

我们的方法是鼓励遵守。当我们发现问题时，我们会采取公平、相称和及时的监管行动，以确保个人的信息权利得到适当的保护。

ICO 如何处理投诉？

如果有人对你的数据共享提出问题，我们将记录并考虑他们的投诉。

数据保护沙龙出品

在考虑你是否遵守了 GDPR 或 DPA 时，特别是在考虑公平性、合法性、透明度和问责制问题时，我们将考虑本守则。

我们将评估你对投诉的最初回应，我们可能会联系你提出一些问题，并为你提供进一步的机会来解释你的立场。我们还可能要求你提供政策和程序、DPIA 和其他相关文档的详细信息。但是，我们希望你对如何履行法律规定的义务负责，因此，你应确保在最初回应个人投诉时，对如何使用他们的个人数据以及如何遵守这些投诉作出完整详细的解释。

如果我们认为你未能（或未能）遵守 GDPR 或 DPA，我们有权采取强制措施。这可能要求你采取措施使你的操作符合要求，或者我们可能决定罚款。

ICO 的执法权力是什么？

我们有各种权力对违反 GDPR 或 DPA 采取行动。在执行 GDPR 和 DPA 时，我们有法定义务考虑本守则的规定。

我们可以使用的工具包括评估通知、警告、谴责、强制执行通知和处罚通知（行政罚款）。对于严重违反数据保护原则的情况，我们有权处以 2000 万欧元或全球年营业额的 4%的罚款，以较高者为准。

根据我们的监管行动政策，我们采取了基于风险的执法方法。我们的目标是创造一种环境，一方面保护数据主体，同时确保企业能够在数字时代高效运营和创新。我们将一如既往地坚持法律，同时确保商业企业不受繁文缛节的约束，或担心制裁将被不适当地使用。

这些权力在 ICO 网站 www.ico.org.uk 上详细列出。

【立法中的相关条款】

See GDPR Articles 12-22 and Recitals 58-72 (external link) See DPA 2018 section 129-164 and schedule 12 (external link)

【本守则以外的延伸阅读】

What we do
Make a complaint
Regulatory Action Policy
Guide to the ICO Sandbox - beta phase

数据保护官办公室出品

附件 A：数据共享清单

- 这些将在最终出版阶段之前添加。

附录 B：模板数据共享请求和决策表

- 这些将在最终出版阶段之前添加。

数据保护官沙龙出品

附录 C：数据保护原则

一般数据处理的数据保护原则（即在 DPA 第 2 部分下）是 GDPR 中规定的原则。但是，第 3 部分中适用于执法处理的原则和第 4 部分中适用于情报服务处理的原则存在一些差异。

为了便于参考，我们在下面一一转载。你还应参考 ICO 指南，网址为 www.ico.org.uk。

- GDPR 数据保护原则“
- 2018 年数据保护法第 3 部分：适用于执法处理的原则

GDPR 数据保护原则

第五条 有关处理个人数据的原则

一、个人数据应：

1、.以合法、公平和透明的方式处理数据主体（“合法、公平和透明”）；

2、.为特定的、明确的和合法的目的而收集的，并且不以与这些目的不符的方式进一步处理；为了公共利益、科学或历史研究目的或统计目的而进一步处理以存档目的的，应当按照第 89（1）条，不应视为与初始目的（“目的限制”）不相容；

3.、充分、相关且仅限于与处理目的相关的必要内容（“数据最小化”）；

4、.准确并在必要时保持最新；必须采取一切合理步骤，确保在考虑到个人数据的处理目的后，及时删除或更正不准确的个人数据（“准确度”）；

5、.以不超过处理个人数据所需时间的方式保存数据主体的标识；个人数据可以存储更长的时间，只要个人数据仅用于为公众利益而进行归档处理。第 89（1）条规定的科学或历史研究目的或统计目的，但应实施本法规要求的适当技术和组织措施，以保障数据主体的权利和自由（“存储限制'）；

6.、以确保个人数据适当安全的方式处理，包括使用适当的技术或组织措施防止未经授权或非法处理，防止意外丢失、破坏或损坏（“完整性和保密性”）。

二、控制者应负责并能够证明符合第 1 款（“责任”）

2018 年数据保护法第 3 部分：适用于执法处理的原则

34.控制者概述和一般职责

（1）本章规定了以下六项数据保护原则：-

（a）第 35（1）节规定了第一个数据保护原则（要求处理合法和公平）；

（b）第 36（1）节规定了第二个数据保护原则（要求明确、合法地规定处理目

数据保护官办公出品

的）；

（c）第 37 条规定了第三项数据保护原则（要求个人数据充分、相关且不过度）；

（d）第 38（1）条列出第四项数据保护原则（要求个人数据准确并保持最新）；

（e）第 39（1）条列出第五项数据保护原则（个人数据的保存期限不得超过所需的时间）；

（f）第 40 节规定了第六个数据保护原则（要求以安全方式处理个人数据）。

（2）另外-

（a）第 35、36、38 及 39 条每一条均作出规定，以补充其所关乎的原则，及

（b）第 41 及 42 条就适用于某些类型的加工处理的保障作出规定。

（3）与个人数据有关的控制者员负责并必须能够证明符合本章的规定。

35.第一数据保护原则

（1）第一数据保护原则是，为任何执法目的处理个人数据必须合法和公平。

（2）为任何执法目的而处理个人数据，只有在以法律为基础和以法律为基础的范围内，并且-

（a）数据主体已同意为此目的进行处理，或

（b）为执行主管当局为此目的而进行的任务，有必要进行处理。

（3）此外，如果为任何执法目的进行的处理是敏感处理，则仅在第（4）和（5）款所列的两种情况下允许进行处理。

（4）第一种情况是-

（a）该数据主体已同意为第（2）（a）款所述的执法目的进行处理，及

（b）在进行处理时，总监备有适当的政策文件（见第 42 条）。

（5）第二种情况是-

（a）为执法目的，严格需要进行处理，

（b）该处理符合附表 8 所列的至少一项条件，及

（c）在进行处理时，管制员有适当的政策文件（见第 42 条）。

（6）国务卿可通过规章修订附表 8——

数据保护官沙龙出品

（a）增加条件；

（b）省略规章根据（a）段增加的条件。

（7）第（6）款下的规定受肯定决议程序的约束。

（8）在本节中，“敏感处理”是指-

（a）处理透露种族或族裔、政治观点、宗教或哲学信仰或工会成员身份的个人数据；

（b）为唯一识别个人而处理遗传数据或生物特征数据；

（c）处理与健康有关的数据；

（d）处理有关个人性生活或性取向的数据。

36.第二数据保护原则

（1）第二数据保护原则是-

（a）在任何情况下收集个人数据的执法目的必须明确、合法，以及

（b）如此收集的个人数据不得以与收集目的不符的方式处理。

（2）第二项数据保护原则（b）段受第（3）及（4）款规限。

（3）为执法目的而收集的个人数据，可为任何其他执法目的（不论是由收集这些数据的控权者或由另一控权者）处理，但-

（a）法律授权控制者为其他目的处理数据，以及

（b）处理是必需的，并与该另一目的相称。

（4）为任何执法目的收集的个人数据，除非获得法律授权，否则不得以非执法目的处理。

37.第三数据保护原则

第三数据保护原则是，为任何执法目的处理的个人数据必须充分、相关，且与处理的目的无关。

38.第四数据保护原则

（1）第四数据保护原则是-

（a）为任何执法目的而处理的个人数据必须准确，并在必要时保持最新，以及

数据保护官沙龙出品

（b）必须采取一切合理步骤，确保在顾及处理个人数据的执法目的后，将不准确的个人数据删除或更正，不得延误。

（2）在为任何执法目的处理个人数据时，必须尽可能将基于事实的个人数据与基于个人评估的个人数据区分开来。

（3）在为任何执法目的处理个人数据时，必须在相关和尽可能清楚地区分与不同类别数据主体有关的个人数据，例如-

（a）怀疑已犯或即将犯刑事罪行的人；

（b）被裁定犯刑事罪行的人；

（c）是或可能是刑事罪行受害者的人；

（d）有犯罪数据的证人或其他人。

（4）必须采取一切合理步骤，以确保不准确、不完整或不再是最新的个人数据不会为任何执法目的而传送或提供。

（5）为此目的-

（a）在传送或提供个人数据前，必须核实其质量，

（b）在所有个人数据的传输中，必须包括使接收者能够评估数据的准确性、完整性和可靠性以及数据最新程度的必要信息，以及

（c）如果在传输个人数据后，发现数据不正确或传输非法，必须立即通知接收者

39.第五数据保护原则

（1）第五项数据保护原则是，为任何执法目的处理的个人数据的保存时间不得超过处理目的所需的时间。

（2）必须制定适当的时限，定期审查是否需要为任何执法目的持续储存个人数据。

40.第六数据保护原则

第六项数据保护原则是，为任何执法目的处理的个人数据必须以确保个人数据适当安全的方式进行处理，并采用适当的技术或组织措施（在此原则中，“适当的安全 Y”包括防止未经授权或非法加工以及意外损失、破坏或损坏）。

数据保护官沙龙出品

附录 D：案例研究

公平和透明

为顾客提供隐私信息的超市

•超级市场通过其“忠诚”卡计划、店内闭路电视和付款记录来保存顾客信息。

公司通常不会向第三方披露任何信息，例如出于营销目的。但是，如果它所掌握的信息与警方调查有关，或者是对法院命令的回应，它就会这样做。

超级市场或信用卡计划经营者应向客户提供隐私信息，一般来说，这些信息解释了其将与第三方（如警察）共享计划成员信息的各种情况。

如果超市向警方披露了某一特定计划成员的信息，如果这会损害预防犯罪，则无需通知该个人。

公平和透明

与信用评级机构共享客户详细信息

一家移动电话公司打算与一家信用评级机构共享客户账户的详细信息。

它必须在客户开户时通知他们，它将与信用评级机构共享信息。

信用评级机构需要能够将记录与正确的个人联系起来，因此移动电话公司必须确保收集足够的信息来区分个人，例如出生日期。

参与的组织必须有程序来处理关于他们所共享信息准确性的投诉。

公平和透明；隐私信息

公共部门机构共享数据以提供协调的方法

两个县议会和 19 个相关伙伴组织共享个人信息，以防止曾经或现在面临脱离教育、就业或培训的高风险的年轻人被社会排斥。通过共享信息，合作伙伴组织可以确保采用协调的方法识别和联系每个年轻人，以提供最适当的支持，鼓励他们重返教育、工作或培训领域。

作为制定数据共享协议的一部分，所有合作伙伴都更新了隐私声明，将新的数据共享包括在内，并同意每个组织都将通过其网站以及员工与年轻人之间的通信和对话来进行沟通。

公平和和透明

在使用共享数据进行研究时公平处理数据的义务

当地一所大学希望对当地贫困家庭儿童的学业表现进行研究。该大学希望通过找出哪些孩子有资格获得学生保险金来确定相关的孩子。因此，决定要求当地所有中小学共享这些个人数

数据保护官沙龙出品

据以及过去三年的相关儿童测试结果。

DPA 包含各种条款，旨在促进为研究目的处理个人数据。但是，没有免除公平处理数据的一般义务。有关家庭收入水平或领取福利的资格的数据可以从儿童的学生保险费状况中推断出来。父母和他们的孩子很可能会反对披露这些数据，因为他们认为这些数据很敏感，可能会受到侮辱。关于孩子学习成绩的数据同样敏感。

相反，学校可以代表研究人员确定符合条件的孩子，并联系他们的父母，解释研究是关于什么的，研究人员想要什么数据。学校可能希望获得家长同意共享数据，但可以获得其他合法性基础。

或者，学校可以向研究人员披露匿名数据集或统计信息。

数据共享协议;可归责性

医疗保健信息共享框架

一个县的医疗保健合作伙伴决定制定一个信息共享框架，以规范他们的共享过程，并鼓励机构安全地共享个人数据。该框架通过合法、安全和保密地共享信息，帮助员工遵守数据保护立法。因此，他们能够整合整个县的服务提供，为居民提供更好的护理结果。在一个关键步骤中，合作伙伴将信息治理结合在一起，从而监督开发框架所需的更改。

该框架的主要目的是确保：

- 人们只需讲一次他们的病情，就可以期待更好的服务提供；
- 当地人民对如何共享信息（以及在何种情况下需要征得他们的同意）有明确的指导；
- 专业人员可以在需要时获取所需的信息，从而为当地人民提供更好的结果；良好的决策得到信息共享框架的支持，为员工提供明确的指导；以及
- •以避免不必要的预约和入院。

框架的原则是：

a）确定信息共享的适当合法性基础；

b）提供信息安全的基础和与信息共享相关的法律要求；

c）满足开发和管理信息共享协议（ISA）使用的需要；

d）鼓励个人数据的流动，并在综合团队中开展良好的实践；

e）为全县范围内监测和审查数据流的流程以及合作伙伴服务之间的信息共享提供基础；

f）防止合作伙伴组织非法使用个人数据；

数据保护官沙龙出品

g）减少个人在接受综合服务时重复其病史的需要。

从框架的介绍中获得关键知识

- 员工需要有权对合作伙伴之间的信息共享感到自信。高层领导需要保持可见，给员工共享患者信息的信心。

- 内部文化需要支持。文化需要强有力的价值观和精神支柱。重要的是要建立一种学习文化，这样才能共享和学习错误，而不是轻视错误。这项学习包括为所有使用综合护理记录的工作人员制定正式培训，并得到框架的支持。

- 需要建立透明度，以便集体了解数据将如何共享以及由谁共享。员工需要清楚他们的角色和责任以及共享信息的好处。

- 需要发展一种以简单语言进行适当共享的文化。消息需要简化以避免混淆，术语需要减少。

合法性基础：法律义务；公平透明；个人权利

法律要求的数据共享

法律要求地方当局参与全国范围的反欺诈活动，包括向反欺诈机构披露其雇员的个人数据。这项活动旨在发现地方当局雇员非法声称他们无权享受的福利。

即使法律要求共享，地方当局仍应告知任何受影响的员工，关于他们的数据将被共享，并应解释发生这种情况的原因，除非这会损害诉讼程序。

地方当局应说明将要共享的数据项（姓名、地址和国家保险号码），并提供将与之共享的组织的身份。当地政府没有理由要求员工同意共享，因为法律规定共享可以在未经同意的情况下进行。

地方当局也应该向其雇员明确表示，即使他们反对共享，它仍然会发生。

地方当局应准备调查任何认为自己受到不公平待遇的员工的投诉，例如，他们的记录与同名员工的记录混在一起。

合法性基础；特殊类别数据；公平和透明；问责制

关于医疗数据共享协议的考虑

一个地区的国民保健服务和社会服务的相关部分与该地区的警察部队共享个人信息，以确保与警察接触的精神卫生服务用户得到保护，并获得适当的专家支持。

合作伙伴组织已经制定了一项数据共享协议，以支持他们的联合心理健康政策。根据案件的具体情况，法律依据可以是同意，也可以是为了公共利益而执行的任务。《数据共享协议》明确规定了各合作伙伴在规定其公共职能时所依赖的各种立法，以及在依赖同意时所需满足的规定。由于转介可能需要特殊类别数据，因此他们还确定了第 9 条的条件。《数据共享协议》

数据保护官沙龙出品

提醒各方维护患者及其护理人员和家属的权利和尊严，尽可能让他们参与风险评估，同时确保他们和他人的安全。

数据共享协议；责任制；信息权

公共部门机构共享数据以提供协调的方法

两个委员会及其当地学校和学院、住房供应商、相关社区组织、当地就业中心和职业服务机构之间共享个人信息，以确定已经或面临脱离教育、就业和就业的高风险的年轻人提供就业或培训。通过共享信息，合作组织可以确保采取协调的方式向年轻人提供最适当的支持，鼓励他们重返教育、工作或培训领域。

合伙人使用数据共享协议来阐述其目的、合法性基础和要共享的信息。协议包括一个关于如何处理数据主体权利的部分，以及商定的共享安全标准；合作伙伴还更新了他们的隐私声明。为了确保质量，他们与一个区域性的数据保护从业者小组共享了他们的协议，以获得反馈。还为合作伙伴制定了一个时间表，定期审查协议，以确保协议保持最新并符合目的。

《2017 年数字经济法》规定的数据共享权力

两家公司都从企业中收取年度账目。账目包含与公司相关的关键公司和财务信息，如公司董事的姓名或显示其损益的财务报告数字。然而，同一家公司有机会向这两个组织中的每一个提交不同的账户集。通过在公司内部建立扩展账户和在 HMRC 建立较低的数字，他们将同时提高金融机构和更广泛的政府的信誉，同时减少税收负债。

直到 2018 年，对数据共享的限制阻止了 HMRC 和 House 公司共享公司账户进行比较。然而，随着 2017 年《数字经济法》的出台，提供了一个许可的法律，用于共享信息以打击欺诈。

在共享信息之前， House 公司和 HMRC 开会制定治理和流程：

- 他们将作为试点共享信息。
- 双方设计并商定了数据规范。
- 他们完成了数据保护影响评估，以确保他们考虑到适当性和公平处理。
- 双方签署了信息共享协议。

HMRC 于 2018 年 10 月向公司注册处披露了第一套公司账户信息，这是《数字经济法》规定的第一次数据传输。

该试点试图通过十个确定的数据分析和合规工作流程来解决欺诈问题，每个流程都与表明虚假账户归档和欺诈活动的行为模式有关。这是第一次使用定性分析来获取和比较关键词和短语。。除此之外，该试点还利用公司内部的后台数据来发现公司之间先前隐藏的联系，这是首次与 HMRC 智能相结合。

数据共享试点发现节省了 1460 万英镑，如果数据共享像往常一样嵌入业务，则将进一步

数据保护官方版本

节省了 1 亿英镑。此外，他们还发现公司内部有 3500 多套账户是不正确的，从而提高了登记簿上所保存数据的完整性。

数据保护官沙龙出品

Data protection

Data sharing code of practice

Draft code for consultation

Information Commissioner's Office

Data sharing: a code of practice

Contents

Foreword

A foreword by Information Commissioner Elizabeth Denham will be included in the final version of the code.

Summary

- This is a statutory code of practice made under section 121 of the Data Protection Act 2018. It is a practical guide for organisations about how to share personal data in compliance with data protection legislation. It explains the law and provides good practice recommendations. Following it along with other ICO guidance will help you to: manage risks; meet high standards; clarify any misconceptions your organisation may have about data sharing; and give you confidence to share data appropriately and correctly.

- This code covers the sharing of personal data between organisations which are controllers. It includes when you give access to data to a third party, by whatever means. Data sharing can take place in a routine, scheduled way or on a one-off basis. When needed, data can be shared in an urgent or emergency situation.

- When considering sharing data, you must assess your overall compliance with the data protection legislation. As a first step you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). We recommend you consider following the DPIA process, even where you are not legally obliged to carry one out.

- It is good practice to have a data sharing agreement. It sets out the purpose of the data sharing, covers what is to happen to the data at each stage, sets standards and helps all the parties to be clear about their respective roles. It helps you to demonstrate your accountability under the GDPR.

- When sharing data, you must follow the key principles in data protection legislation.

- The accountability principle means that you are responsible for your compliance with the GDPR or DPA, as appropriate. You must be able to demonstrate that compliance.

- You must identify at least one lawful basis for sharing data from the start.

- You must always share personal data fairly and in a transparent manner. When you share data, you must ensure it is reasonable and proportionate. You must ensure individuals know what is happening to their data unless an exemption or exception applies.

- Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place.

- In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights with ease.

- In order to comply with the lawfulness principle you must identify a lawful basis for your data sharing and ensure your data sharing is lawful in a more general sense.

- Most data sharing, and the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a "competent authority" for specific law enforcement purposes is subject to a different regime under Part 3 of the DPA for Law Enforcement Processing, which provides a separate but complementary framework.

- If a merger or acquisition or other change in organisational structure means that you have to transfer data to a different controller, you must take care. You must ensure you consider data sharing as part of your due diligence.

- The transfer of databases or lists of individuals is a form of data sharing. This may include sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies, and political parties. You are responsible for compliance with the law for the data you receive, and for data that is shared on your behalf. You must make appropriate enquiries and checks in respect of the data, including its source and any consent given.

- If you are considering sharing children's personal data, you must proceed with caution. You should consider the need to protect them from the outset. If the data sharing is of a type likely to result in a high risk to children's rights and freedoms, a DPIA is compulsory.

- In an emergency you should go ahead and share data as is necessary and proportionate.

- The government has devised a framework for the sharing of personal data, for defined purposes across the public sector, under the Digital Economy Act 2017 (the DEA). Data sharing under the DEA powers has to comply with the data protection legislation and with codes of practice that are consistent with this code.

- You should bear in mind ethical factors in addition to legal and technical considerations when deciding whether to share personal data. Data trusts are a relatively recent concept enabling independent third-party stewardship of data.

- The ICO upholds information rights in the public interest. In the context of data sharing, our focus is to help you carry out data sharing in a compliant way. We will always use our powers in a targeted and proportionate manner, in line with our regulatory action policy.

About this code

At a glance

This is a statutory code of practice prepared under section 121 of the Data Protection Act 2018.

It is a practical guide for organisations about how to share personal data in compliance with data protection legislation. It explains the law and provides good practice recommendations. Following it along with other ICO guidance will help you to: manage risks; meet high standards; clarify any misconceptions you may have; and give you confidence to share data appropriately and correctly.

In more detail

What is the status of this code?

This is a statutory code of practice prepared under section 121 of the Data protection Act 2018 (DPA):

> "The Commissioner must prepare a code of practice which contains—
>
> (a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and
>
> (b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data."

It was laid before parliament on [date] and issued on [date] under section 125 of the DPA. It comes into force on [date].

The code contains practical guidance on how to share data fairly and lawfully, and how to meet your accountability obligations. It does not impose any additional barriers to data sharing, but will help you comply with your legal obligations under the GDPR and the DPA.

It also contains some optional good practice recommendations, which do not have the status of legal requirements but aim to help you adopt an effective approach to data protection compliance.

In accordance with section 127 of the DPA, the Commissioner must take the code into account when considering whether you have complied with your data protection obligations in relation to data sharing. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR or the DPA.

The code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.

What happens if we don't comply with the code?

If you don't comply with the guidance in this code, you may find it more difficult to demonstrate that your data sharing is fair, lawful and accountable and complies with the GDPR or the DPA.

If you process personal data in breach of this code and this results in a breach of the GDPR or the DPA, we can take action against you.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to €20 million or 4% of your annual worldwide turnover, whichever is higher.

There is no penalty if you fail to adopt good practice recommendations, as long as you find another way to comply with the law.

For more information, see the separate chapter on enforcement of this code.

What is the status of 'further reading' or other linked resources?

Any further reading or other resources which are mentioned in or linked from this code do not form part of the code. We provide links to give you helpful context and further guidance on specific issues, but there is no statutory obligation under the DPA for the Commissioner or the courts to take it into account (unless it is another separate statutory code of practice).

However, where we link to other ICO guidance, that guidance will inevitably reflect the Commissioner's views and inform our general approach to interpretation, compliance and enforcement.

Relevant provisions in the legislation

See DPA 2018 sections 121, 125 and 127

How should we use this code?

The code covers data sharing by organisations subject to the processing regimes under the GDPR and Part 2 of the DPA, and also the Law Enforcement (LE) regime in Part 3 of the DPA. Most data sharing is likely to be under the GDPR and Part 2 of the DPA, but where provisions differ we clarify this as far as possible. There is a separate chapter in this code on LE processing, that describes the differences in more detail, but controllers carrying out that type of processing should still read the whole of the code. The code does not cover data sharing under the Intelligence Services regime in Part 4 of the DPA.

The code is complementary to other ICO guidance and codes of practice relating to data protection. It assumes knowledge of key data protection terms and concepts. While the code stands alone as your guide to data sharing, it does not seek to reproduce other ICO guidance and you might need at times to refer out to guidance on the ICO website at www.ico.org.uk. This might be for an overview of data protection law or for more detailed guidance on

specific concepts, obligations and rights. The code will highlight particular instances when it would be useful for you to refer to such guidance.

In particular, you will find it helpful to use the Data Protection Impact Assessment (DPIA) process along with this code when considering sharing data. Some or all of the DPIA questions are likely to help you when you are assessing whether it is appropriate to share data, and whether it would be in compliance with the law. You can find more on DPIAs later in the code.

Further reading outside this code

ICO's Guide to Data Protection
Guide to Law Enforcement Processing

Who is this code for?

The code is mainly aimed at organisations which are controllers sharing data subject to the GDPR and under the general data processing provisions of Part 2 of the DPA.

Controllers are defined under Article 4 of the GDPR. The code is also aimed at controllers sharing data under the Law Enforcement Processing (LE) regime (Part 3 DPA). There is a separate chapter for LE Part 3 data sharing. If you are one of these controllers, you should still read the whole of this code, which distinguishes between the regimes where appropriate.

Much of the advice is applicable to public, private and third sector organisations. Some of the code is necessarily focused on sector-specific issues. However, the majority of the code applies to all data sharing, regardless of its scale and context.

Reading and understanding the code and adopting its practical recommendations will give you confidence to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

The code will help you identify what you need to consider before you share personal data and clarify when it is appropriate for you to do so.

Relevant provisions in the legislation

See GDPR Articles 4(7) and 4(8)
See DPA 2018 section 3(9)

Further reading outside this code

Controllers and processors under the GDPR

What is the purpose of this code?

This code provides practical guidance for organisations about sharing personal data in compliance with data protection legislation. It explains the law and promotes good practice.

Many organisations using this code will have already shared data under the former data protection regime. This code should give you the knowledge and the confidence you need to continue sharing data under the GDPR and the DPA.

The code:

- updates and reflects key changes in data protection law since the last code was published (in particular from the GDPR and the DPA);
- explains new developments in technology and their impact on data protection;
- references new areas for you to consider; and
- helps you to manage risks in sharing data, which are magnified if the quantity of data is large.

Common concerns about data sharing

The code also clears up misconceptions about data sharing and barriers to sharing. The arrival of the GDPR and DPA in 2018 appears to have caused some concern amongst organisations about data sharing. However, many of the requirements of data protection law simply place on a statutory footing the good practice that you will already have followed, or plan to follow.

For example:

Misconception
Data protection prevents us from sharing data.

Reality
Data protection does not prevent data sharing, as long as you approach it in a sensible and proportionate way. This code helps you to balance the risks and benefits and implement data sharing if it is:

- in the public interest; or
- proportionate, in the case of sharing for commercial reasons.

Misconception
The GDPR presents additional barriers to sharing data.

Reality
This is mistaken. Whilst the GDPR and DPA have changed some aspects of the law on data protection, they do not prevent you from data sharing. If you were able to share data lawfully under the former data protection regime, it is likely that you are able to continue to do so under the new data protection legislation, even though there are some differences, which we explain in this code. Under the GDPR you must be certain you are accountable for your decision to share.

Misconception
There is little benefit to be gained from data sharing.

Reality
Data sharing can bring benefits to your organisation, individuals and society at large. Done well, it can help government and commercial organisations to deliver modern, efficient services which better meet people's needs and make their lives easier. It can also identify people at risk and address problems before they have a significant adverse impact.

Misconception
We can only share data with people's consent.

Reality
Not always. You can usually share without consent if you have a good reason to do so. However, there are some cases where the impact on individuals might override your interests in sharing, in which case you might need to ask for their consent.

Misconception
We can't share data in an emergency.

Reality
You may be able to do so. And in an emergency scenario you should do whatever is necessary and proportionate. Please see our section on this topic later in the code.

The benefits of data sharing

The code also highlights the benefits that sharing personal data can bring to everyone: society, organisations, and individuals, whether as citizens or consumers. Data sharing, done in accordance with the law and good practice, can help government and other organisations deliver modern, efficient services and can make everyone's lives easier. Conversely, not sharing data can mean that everyone fails to benefit from these opportunities; and in some instances the chance is missed to assist citizens in need, whether in urgent or longer term situations.

The benefits for you in adopting the code's recommendations may include:

- better compliance with the law;
- better protection for individuals whose data is being shared;
- greater trust in you by the public, whose data you may want to share;
- an improved understanding of whether and when it is appropriate to share personal data;
- greater confidence within your organisation that you are sharing data appropriately and correctly;
- the confidence to share data in a one-off situation or in an emergency; and
- a reduced reputational risk when sharing data.

Example

A local area set up an integrated care record to share patient records between health and social care staff. This resulted in:

- a more holistic picture about a patient's health;
- coordinated and safer care across the region;
- better decision making around a patient's care; and
- patients only having to tell their story once.

Example

A hospital emergency department and the local GPs introduced a data sharing process to enable the hospital's treating clinicians to have 24 hour secure access to the patient's GP record. The benefits of this arrangement included:

- better informed clinical decisions on how patients are treated based on previous medical history and current treatment plans;
- safer care by identifying current patient medications and allergies;
- a reduction in unnecessary emergency admissions and duplicate tests;
- removal of the burden on GPs having to print this information and provide it to the hospital; and
- improved patient experience and reduced service costs as clinicians and patients no longer had to wait for the information to arrive by other means.

Example

Several health professionals from different organisations were involved in providing health and social care to a group of older adults. By exchanging information about recent changes in behaviour from one of the service users, they identified a pattern of evidence indicating that the person might be a victim of abuse. They shared this information with the person's social worker for further investigation.

Data sharing covered by this code

At a glance

This code covers the sharing of personal data between organisations which are controllers. It includes when you give access to data to a third party, by whatever means. Data sharing can take place in a routine, scheduled way or on a one-off basis. When needed, data can be shared in an urgent or emergency situation.

In more detail

Data sharing covered by this code

There is no formal definition of data sharing within the legislation, although the scope of this code is defined by section 121 of the DPA as "the disclosure of personal data by transmission, dissemination or otherwise making it available". This means giving personal data to a third party, by whatever means; and includes when you give a third party access to personal data on or via your IT systems.

For the purposes of this code, it does not include sharing data with employees, or with processors.

The following non-exhaustive list shows what data sharing could cover:

- a reciprocal or one-way exchange of data between organisations;
- an organisation providing another organisation with access to personal data on its IT system for a specific research purpose;

- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;
- data sharing on a routine, systematic basis for an established purpose;
- one-off, exceptional or ad hoc data sharing; and
- one-off data sharing in an urgent or emergency situation.

Examples of real-life data sharing activities

- a primary school passed details about a child showing signs of harm to the police or a social services department;
- the police passed information about the victim of a crime to a counselling charity;
- a retailer provided customer details to a payment processing company;
- the police and immigration authorities exchanged information about individuals thought to be involved in serious crime;
- a supermarket gave information about a customer's purchases to the police;
- a local authority disclosed personal data about its employees to an anti-fraud body;
- two neighbouring health authorities shared information about their employees for fraud prevention purposes;
- a school provided information about its pupils to a research organisation; and
- a multi-agency network group regularly exchanged information about individuals for safeguarding or social care purposes.

This code only applies to sharing personal data. Some sharing doesn't involve personal data. For example if an organisation is sharing information that cannot identify anyone (anonymous information; please refer to the ICO website www.ico.org.uk if you need more information about anonymisation or pseudonymisation). Neither the GDPR, the DPA, nor this code of practice, applies to the sharing of information that does not constitute personal data.

It is common to consider data sharing as falling into two main different types of scenario:

- routine data sharing, sometimes known as "systematic" data sharing, where the same data sets are regularly shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for a purpose that is ad hoc or unexpected or due to an urgent situation or emergency.

Different approaches apply to these two scenarios, and the code reflects this. Most of the code concentrates on routine data sharing.

Routine data sharing

This is data sharing done in a routine, pre-planned way. It will generally involve the sharing of data between organisations for an established purpose, perhaps the same sets of data, at regular, scheduled intervals.

A variation on this might be a group of organisations making an arrangement to share or pool their data for specific purposes, again on a regular basis.

If you are carrying out this type of data sharing you should establish rules and agree procedures in advance.

Ad hoc or one-off data sharing

Sometimes organisations may decide, or are asked, to share data in situations which are not covered by any routine arrangement or agreement. It is still possible to share data in this type of scenario. We recommend that you make plans to cover such contingencies.

Sometimes you may have to make a decision quickly about data sharing in conditions of real urgency, or even in an emergency situation. You should not be put off from data sharing in a scenario like this; in an urgent situation you should do what is necessary and proportionate.

Data pooling

Data pooling is a form of data sharing where organisations decide together to pool information they hold and make it available to each other, or to different organisations.

The organisations responsible for the data sharing would be regarded as joint controllers under Article 26 of the GDPR.

Data sharing between controllers

This code of practice focuses on the sharing of personal data between controllers, ie where separate or joint controllers determine the purposes and means of the processing of personal data, as defined in GDPR Article 4(7).

Sharing data with a processor

If a controller asks another party to process personal data on its behalf for the purposes of the GDPR the other party is a "processor", as defined in Article 4(8). The GDPR draws a distinction between a controller sharing personal data with another controller, and a processor processing personal data on behalf of a controller.

Article 28 of the GDPR lays down requirements that must be in place between a controller and processor, in order to protect the rights of the data subject. These requirements include a written contract and guarantees about security. Under the GDPR a processor must only process personal data on documented instructions from the controller. A processor has its own liabilities and responsibilities both under the contract and under the GDPR. This type of arrangement is outside the scope of this code. For more details, you should refer to the guidance on the ICO website www.ico.org.uk.

Further reading outside this code

Contracts and liabilities between controllers and processors
Key definitions: controllers and processors
Guide to the GDPR: controllers and processors

Relevant provisions in the legislation

See GDPR Articles 4, 26 and 28 and Recitals 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 81 and 82 (external link)
See DPA 2018 section 121 (external link)

Deciding to share data

At a glance

When considering sharing data, you must consider your overall compliance with the data protection legislation. As a first step you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). We recommend you consider following the DPIA process, even where you are not legally obliged to carry one out.

In more detail

What do we need to do?

When considering sharing data, you must consider your overall compliance with the data protection legislation. As a first step, you should decide whether you need to carry out a Data Protection Impact Assessment (DPIA). You have to do this in order to demonstrate your compliance with the DPIA provisions. Even if you are not legally obliged to carry one out, we recommend you consider following the DPIA process.

Do we need to do a DPIA?

- You must do a DPIA for data sharing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.
- The GDPR gives examples of processing that require a DPIA:
    - where the use of innovative technology is likely to result in a high risk to the rights and freedoms of individuals;

    - automated decision-making (including profiling) resulting in a significant legal effect;
    - large-scale processing of special category data or criminal offence data; and
    - large-scale systematic monitoring of public spaces.

- It is also good practice to do a DPIA for any other major project which involves sharing personal data.
- In our view, examples of processing requiring a DPIA that might be relevant to data sharing also include:

    - data matching;
    - invisible processing; (there is more detail on this in the ICO's DPIA guidance); and
    - processing records where there is a risk of harm to individuals in the event of a data breach, such as whistleblowing or social care records.

There are instances other than the GDPR where a DPIA is obligatory; for example, pilots under the Digital Economy Act 2017.

In order to help you determine whether you need to carry out a DPIA you:

- can use our screening checklists on the ICO website; and
- should read the guidance on DPIAs on the ICO website www.ico.org.uk.

You should regard it as good practice to do a DPIA if you have any major project that involves the disclosure of personal data, or any plans for routine data sharing, even if there is no specific indicator of likely high risk.

If you have taken into account the nature, scope, context and purposes of the sharing and you are confident that the type of data sharing you have in mind is unlikely to result in high risk, you may not be legally required to do a DPIA. Nonetheless you can use the DPIA process as a flexible and scalable tool to suit your project.

What factors should we consider?

There are some practical and legal factors you should consider when you are deciding whether to share data.

This includes asking yourself the following questions:

- **What is the sharing meant to achieve?**
  When deciding whether to enter into an arrangement (whether one-off or ongoing and repeated) to share personal data (either as a provider, a recipient or both) you need to identify the objective(s) that the sharing is meant to achieve. You must have one or more clear objectives. This will allow you to work out what data you need to share and with whom. You must document this, and it would be good practice to do so in a data sharing agreement (also sometimes known as an information sharing agreement).

- **What information do we need to share?**
  You should only share the specific personal data needed to achieve your objectives. For instance, you might need to share somebody's current name and address, but not other information you hold about them.

- **Could we achieve the objective without sharing the data or by anonymising it?**
  If you can reasonably achieve the objective in another less intrusive way, you should not process the personal data. For example, where you could instead do this by sharing data that has been rendered anonymous (to which the GDPR doesn't apply) then you should do so, as it would be inappropriate to share the personal data itself in this context.

- **What risks does the data sharing pose to individuals?**
  Consider, for example, if any individual is likely to be harmed by it in any way, including physical, emotional, economic and social harms. Is any individual likely to object? Could it undermine individuals' trust in the organisations that keep records about them?

- **Is it right to share data in this way?**
  You should consider the potential benefits and risks, to both society and individuals, of sharing the data. Where appropriate, ethics should form a part of those considerations. Please also see the section on this later in the code. The proportionality of the data sharing exercise should be central to your analysis.

- **What would happen if we did not share the data?**

You should also assess the likely results of not sharing the data; this can itself be harmful.

- **Are we allowed to share the information?**
  Check whether there is any statutory bar or other restriction on sharing the data.

- **Who requires access to the shared personal data?**
  You should employ "need to know" principles, meaning that you should only share data to the extent that it is proportionate to do so:
  - other organisations should only have access to your data if they need it; and
  - only relevant staff within those organisations should have access to the data.

  As part of this, you should consider any necessary restrictions you may need to impose on the onward sharing of data with third parties.

- **When should we share it?**
  You must document this, for example whether the sharing should be an ongoing, routine process or whether it should only take place in response to particular events, and detail what these are.

- **How should we share it?**
  What are the processes for sharing the data? This must include security considerations and procedures around the transmission of data, and access to it by all those involved. For more on this, see later in the code.

- **How can we check the sharing is achieving its objectives?**
  You should refer to your objectives. What are you attempting to achieve by sharing this data? Being clear about this will help you measure whether the sharing has been successful. Then you can judge whether the data sharing is still appropriate, and whether the safeguards still match the risks.

- **Do we need to review the DPIA?**
  You must keep the risks of all data sharing arrangements under review, as with any form of data processing. If there is a significant change in the operation, such as the introduction of new technology, or a widening of scope, you should consider this as a trigger for a review of any existing DPIA (or PIA as it was formerly known), or for carrying out a

new assessment.

Sharing data outside the EEA

Will any of the data be transferred outside the European Economic Area (EEA)?

We will provide more guidance on this in due course. In the meantime you should refer to the guidance on the ICO website www.ico.org.uk for the latest position.

Relevant provisions in the legislation

See GDPR Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95
See DPA 2018 section 207 (external link)

Further reading outside this code

Data protection impact assessments
Detailed guidance on DPIAs
DPIA suggested template
DPIA checklists
International transfers
Data protection and Brexit

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB. The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Data sharing agreements

At a glance

It is good practice to have a data sharing agreement. It sets out the purpose of the data sharing, covers what is to happen to the data at each stage, sets standards and helps all the parties to be clear about their respective roles. It helps you to demonstrate your accountability under the GDPR.

In more detail

A data sharing agreement between the parties sharing and receiving data can form a major part of your compliance with the accountability principle of the GDPR. Sometimes a data sharing agreement is called an information sharing agreement, a data or information sharing protocol, or a personal information sharing agreement. It is good practice to have one in place.

What are the benefits of a data sharing agreement?

A data sharing agreement:

- helps all the parties to be clear about their respective roles;
- sets out the purpose of the data sharing;
- covers what is to happen to the data at each stage; and
- sets standards.

It should help you to justify your data sharing and to demonstrate that you have been mindful of, and have documented, the relevant compliance issues.

There is no set format for a data sharing agreement; it can take a variety of forms, depending on the scale and complexity of the data sharing in question. Since a data sharing agreement is a set of common rules binding on all the

organisations involved in a data sharing initiative, you should draft the agreement in clear, concise language that is easy to understand.

Drafting and adhering to an agreement does not in itself provide you with any form of legal indemnity from action under the data protection legislation or other law. However The ICO will take this into account if it receives a complaint about your data sharing.

What should we include in a data sharing agreement?

In order to adopt good practice and to comply with the data protection legislation, the ICO expects you to address a range of questions in a data sharing agreement, including:

What is the purpose of the data sharing initiative?

Your agreement should explain:

- why the data sharing initiative is necessary;
- the specific aims you have; and
- the benefits you hope to bring to individuals or to society more widely.

You should document this in precise terms so that all parties are absolutely clear about the purposes for which they may share or use the data.

Which other organisations will be involved in the data sharing?

Your agreement should identify clearly all the organisations that will be involved in the data sharing and should include contact details for their Data Protection Officer (DPO) and other key members of staff. It should also contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.

Are we sharing data along with another controller?

Where you are acting with another controller as joint controllers of personal data within the meaning of Article 26 of the GDPR, you are required to set out your responsibilities in an "arrangement". This may be done by means of a data sharing agreement. Under the transparency requirements of the GDPR you must make the essence of the agreement available to individual data

subjects. We recommend you do this in the privacy information you give to them.

What data items are we going to share?

Your agreement should explain the types of data you are intending to share with the organisations stated above. This may need to be quite detailed, because in some cases it will be appropriate to share only certain details held in a file about an individual, omitting other, more sensitive, material. In some cases it may be appropriate to attach "permissions" to certain data items, so that only particular members of staff are allowed to access them, for example ones who have received appropriate training.

What is our lawful basis for sharing?

You need to explain clearly your lawful basis for sharing data. If you are a public sector organisation, you should also set out the legal power under which you are allowed to share it.

If you are using consent as a lawful basis for disclosure, then your agreement could provide a model consent form. You should also address issues surrounding the withholding or retraction of consent.

Is there any special category data or sensitive data?

You must document the relevant conditions for processing, as appropriate under the GDPR or the DPA, if the data you are sharing contains special category data or criminal offence data under the GDPR, or sensitive data within the meaning of Parts 2 or 3 of the DPA.

What about access and individual rights?

You should set out procedures for compliance with individual rights. This includes the right of access to information as well as the right to object and requests for rectification and erasure. The agreement must make it clear that all controllers remain responsible for compliance even if you have processes setting out who should carry out particular tasks.

For example, the agreement should explain what to do when an organisation receives a request for access to shared data or other information, whether it is under the data protection legislation, FOIA or the EIR. In particular, it should ensure that one staff member (generally a DPO) or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily.

For joint controllers, Article 26 requires you to state in the agreement which controller is responsible for responding to individuals who exercise their data subject rights, although individuals may choose to contact any controller.

You will have to take decisions about access on a case by case basis.

For public authorities, the agreement should also address the inclusion of certain types of information in your FOIA publication scheme.

What information governance arrangements should we have?

Your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing:

- have detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed;
- make sure that the data they are sharing is accurate, for example by requiring a periodic sampling exercise;
- are using compatible datasets and are recording data in the same way. The agreement could include examples showing how particular data items should be recorded, for example dates of birth;
- have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement;
- have procedures for dealing with access requests, complaints or queries from members of the public;
- have a timescale for assessing the ongoing effectiveness of the data sharing initiative and the agreement that governs it; and
- have procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

What further details should we include?

It is likely to be helpful for your agreement to have an appendix or annex, including:

- a summary of the key legislative provisions, for example relevant sections of the DPA, any legislation which provides your legal power for data sharing and links to any authoritative professional guidance;
- a model form for seeking individuals' consent for data sharing; and
- a diagram to show how to decide whether to share data.

You may also want to consider including a data sharing:

- request form; and
- decision form.

You can find examples of these in Annex B of this code.

When should we review a data sharing arrangement?

You should review your data sharing agreement on a regular basis because changes in circumstances or the rationale for the data sharing may arise at any point.

You should ask yourself the following key questions regularly:

- Is the data still needed? It's essential that you factor any new developments into your regular review of the data sharing arrangement to ensure that you can still justify the sharing. You may find you have achieved the aim of the data sharing and so no further sharing is necessary. On the other hand, you may find that the data sharing is making no impact upon your objective and therefore the sharing is no longer justified. If you cannot justify it, you should stop.
- Have you proactively communicated any changes to your data sharing arrangement to the people concerned?
- Do your privacy information and any data sharing agreements still explain the data sharing you are carrying out accurately?
- Are your information governance procedures still adequate and working in practice? All the organisations involved in the sharing should check whether:
    - it is necessary to share personal data at all, or you could use anonymised information instead;

    - you are only sharing the minimum amount of data and that the minimum number of organisations, and their staff members, have access to it;
    - the data you are sharing is still of appropriate quality;
    - all the organisations involved in the sharing are still applying the retention periods correctly;
    - all the organisations involved in the sharing have attained and are maintaining an appropriate level of security; and
    - staff are properly trained and are aware of their responsibilities for any shared data they have access to.
- Are you still providing people with all their individual rights under the GDPR or DPA as appropriate?
- Are you responding to people's queries and complaints properly and are you analysing them to make improvements to your data sharing arrangements?

Data protection principles

When sharing data, you must follow the key principles in data protection legislation. There are some differences between the principles in the respective pieces of legislation:

- Article 5 of the GDPR; and
- Sections 34-40 of Part 3 of the DPA for law enforcement processing.

We have reproduced the principles in Annex C to this code, and you should refer to the detailed guidance on the ICO website at www.ico.org.uk.

Further reading outside this code

Guide to the GDPR: principles
Guide to Law Enforcement processing

Accountability

At a glance

The accountability principle means that you are responsible for your compliance with the GDPR or DPA, as appropriate. You must be able to demonstrate that compliance by:

- maintaining documentation of all your data sharing operations;
- implementing appropriate security measures;
- recording any personal data breaches, and reporting them where necessary;
- carrying out data protection impact assessments (DPIAs) for any data sharing that is likely to result in high risk to the interests of individuals; and
- appointing a data protection officer (DPO) when appropriate.

You should review all your accountability measures regularly.

In more detail

What is the accountability principle?

Accountability is a legal requirement for data sharing; it is one of the principles applicable to general data processing under the GDPR, Part 2 of the DPA and law enforcement processing under Part 3.

The accountability principle requires that if you are involved in a data sharing arrangement you are responsible for your compliance with the GDPR or DPA as

appropriate, and you must be able to demonstrate that compliance. As part of this, and where proportionate, you must put in place a data protection policy, adopting a "data protection by design and default" approach which will help you comply with the data protection legislation and good practice whenever you process data.

There is a general obligation to evidence your compliance and justify your approach, so you should adopt additional measures as necessary. A data sharing agreement would be one example of good practice to demonstrate your accountability. If you are unable to justify your approach, an accountability breach is likely, regardless of the outcome.

The importance of the accountability principle cannot be overstated. To be effective, you have to embed the message of accountability in the culture and business of your organisation, from Board level through all your employees.

What is data protection by design and default?

"Data protection by design and default" is a legal obligation requiring you to put in place appropriate technical and organisational measures to:

- implement the data protection principles in an effective manner; and
- safeguard individual rights.

This means that you have to hard-wire data protection throughout your data sharing processes, plans and activities.

There is more on technical measures relating to security in the chapter on security. Other technical measures include those designed to evidence compliance with other obligations. For example, technical measures that:

- give evidence of consent, including a timestamp as to information provided at the time; and
- ensure that withdrawals of consent, or objections, are processed properly and details are suppressed effectively.

What documentation do we need to keep?

Under Article 30 of the GDPR, larger organisations are required to maintain a record of their processing activities. Therefore you must ensure you document any data sharing you undertake, reviewing it regularly.

Documenting this information is a practical way of taking stock of your data sharing. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the GDPR, such as making sure that the information you hold and share about people is accurate and secure.

As well as your record of data sharing and other processing activities under Article 30, under Article 5(2) and Article 24 you also need to document other things to show your compliance with the GDPR. You need to keep sufficient documentation to be able to demonstrate your compliance with all principles, obligations and rights. As part of this, you must keep records of consent and of any personal data breaches.

You must document together all aspects of the data sharing, and other aspects of your compliance with the data protection legislation, such as your record of the lawful basis for processing and the privacy information you provide.

What is the role of the Data Protection Officer (DPO) in a data sharing arrangement?

If your organisation has a DPO, they should be closely involved from the outset in any plans to enter into a data sharing arrangement.

DPOs play an important role while a data sharing arrangement is under way. Since there will be a number of organisations involved, each of you will have your own responsibilities for the data you disclose or have received. Often the purpose of a data sharing arrangement involves very sensitive issues. In each of the organisations, the DPO advises everyone on information governance, ensures compliance with the law, and provides advice to staff faced with decisions about data sharing. They may also be a contact point for individuals to exercise their rights.

Example

A police intelligence database on gangs in an area (the gangs database) had been shared by the police with the local authority. The council went on to share it inappropriately with a number of organisations.

Shortly afterwards there were incidents of gang violence in the area and some victims had featured in the gangs database. Whilst it was not possible to establish a causal connection to the data breach, it was obvious that there would have been a risk of distress and harm when this type of sensitive data was not kept secure.

In this case it was apparent that it was unfair and excessive for the council to have shared the unredacted database with a large number of people and other organisations. It should have realised that there was an obvious risk in doing so.

There is a national concern about the need to tackle gang crime, and it is widely recognised that this is a challenge for public authorities. Data sharing has an important role to play in tackling this challenge; however it has to be carried out in compliance with the law. Data must be processed lawfully, fairly, proportionately and securely. However data protection law is not a barrier to data sharing.

To help to prevent such incidents happening, organisations processing sensitive data should have in place policies, processes and governance as well as training for staff. Conducting a data protection impact assessment (DPIA) is one way of helping an organisation to ensure it is complying with the law. This data sharing code also provides practical guidance.

Example

A health care organisation provided an out-of-hours emergency telephone service. As calls could be received about clients' welfare, it was essential that advisors had access to some personal data about the organisation's clients to carry out their role.

A call was taken by a new advisor late one evening by someone identifying themselves as a police officer and requesting the address of one of its clients. The organisation had protocols to follow about sharing data to third parties, and it was mandatory that all new advisors underwent this training on appointment. The advisor therefore knew the procedure to follow to determine whether or not they could share this information.

Relevant provisions in the legislation

See GDPR Articles 5(2), 25, 28,29,30,31,32,34,35, 38, 39 and Recitals 39, 81-83 (external link)
See DPA Part 3

Further reading outside this code of practice

ICO guidance on DPIAs, DPOs, documentation and accountability

Lawful basis for sharing personal data

At a glance

You must identify at least one lawful basis for sharing data from the start. You must be able to show that you considered this beforehand, in order to satisfy the accountability principle.

In more detail

What are the provisions on lawful basis?

You must identify at least one lawful basis for sharing data, from a number of provisions which are different for the GDPR and for Law Enforcement Processing under Part 3 of the DPA. This is known as a lawful basis for processing, and at least one must apply from the start of your data sharing. You must be able to show that you considered this before you started data sharing, in order to satisfy the accountability principle in the GDPR and Part 3 of the DPA. And without at least one lawful basis for processing, any data sharing you do will be in breach of the first principle in each piece of legislation.

Lawful basis under the GDPR

For data sharing under the GDPR (and under Part 2 of the DPA), there are six lawful bases for processing, contained in Article 6. In summary they are as follows. For more details, you should refer to the ICO website at www.ico.org.uk.

(a) Consent: the individual has given their clear consent for you to share their personal data for a specific purpose.

(b) Contract: the sharing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the sharing is necessary for you to comply with the law (other than contractual obligations).

(d) Vital interests: the sharing is necessary to protect someone's life.

(e) Public task: the sharing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the sharing is necessary for your legitimate interests or those of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, especially where the individual is a child. You cannot use legitimate interests as your lawful basis if you are a public authority processing data to perform your official tasks.

How do we determine which lawful basis is appropriate?

You should consider carefully all the background details to your plans for data sharing. Relevant factors include:

- the nature of the data;
- your purpose for sharing the data;
- the context of the sharing; and
- your relationship with the individual(s).

Most of the lawful bases in the GDPR require the processing to be "necessary" for a specific purpose. This assessment links to the DPIA process, which requires you to consider both necessity and proportionality. Ask yourself:

- do your plans help to achieve your purpose?
- is there any other reasonable way to achieve the same result?

"Necessary" means that the data sharing must be more than just useful, or standard practice. It must be a targeted and proportionate approach that is objectively necessary to achieve your stated specific purpose. If you can reasonably achieve the purpose by some other less intrusive means, or by sharing less information, you won't have a lawful basis for the data sharing and you should not go ahead.

You should decide which lawful basis applies before you start processing any personal data. It's important to choose the appropriate lawful basis from the start. You should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.

You must tell individuals about your lawful basis for sharing their data in your privacy notice, along with the other details you have to provide. Please see later in the code for details about privacy information.

For more information on how to determine which lawful basis is suitable for the data sharing you have in mind, please refer to the guidance on the ICO website at www.ico.org.uk.

What do we need to do if we are relying on legitimate interests as our lawful basis?

If you are relying on legitimate interests as your lawful basis for disclosing data to a third party, you must carry out a three-part test known as a legitimate interests assessment (LIA). This test considers some of the same questions as a DPIA, considering the necessity of the data sharing as well as individual rights. There is more information on this on the ICO website at www.ico.org.uk.

What do we need to do in respect of special category data and criminal offence data?

Some data sharing arrangements involve special category data. If you are sharing special category data under the GDPR, you must identify both a lawful basis for the sharing and an additional condition for doing so. Article 9(1) prohibits the processing of special category data but Article 9(2) lists conditions allowing its processing in certain circumstances. Some of the conditions listed in Article 9(2) are subject to conditions in Part 1 of Schedule 1 of the DPA. In summary these are around the following areas:

- employment;

- social security and social protection;
- health and social care;
- public health; and
- archiving, research and statistics.

If the data you plan to share concerns criminal convictions, criminal offences or related security measures, under Article 10 of the GDPR you must identify a lawful basis for general processing and either have "official authority" or meet a separate condition for processing this data under Schedule 1 of the DPA.

How do we determine which lawful basis is appropriate under Part 3 of the DPA - Law Enforcement Processing?

For data sharing carried out under the Law Enforcement provisions, it is only lawful "if and to the extent that it is based on law" and either:

- the individual has consented to the data sharing for that purpose; or
- the data sharing is necessary for the performance of a task carried out for that purpose by a competent authority.

What do we need to do about sensitive processing under Part 3 of the DPA?

For law enforcement processing the term "sensitive processing" is similar to special category data. If you want to share any data that falls under this heading, you must meet the requirements of one of the two cases set out in section 35 of Part 3 of the DPA:

<u>The first case</u>

- specific consent by the data subject to that data sharing for the law enforcement purpose in question; and
- when the sharing is carried out, you must have an "appropriate policy document" as defined in section 42.

<u>The second case</u>

- the processing is strictly necessary for law enforcement purposes;
- the processing meets at least one Schedule 8 condition; and

- when the sharing is carried out, you have an appropriate policy document.

Relevant provisions in the legislation

See GDPR Articles 6(1)(c), 6(1)(e), 6(1)(f), 6(3), 9(2), 13(1)(c), 14(1)(c), and Recitals 39, 41, 45, 47-49, 50, 51
See DPA 2018 sections 7, 8, 10, 11, 35, 42 and Schedules 1 (paras 6 and 7) and 8.

Further reading outside this code of practice

Lawful basis for processing
Lawful basis interactive guidance tool
Legitimate interests
Legitimate interests assessment
Guide to law enforcement processing

Fairness and transparency in data sharing

At a glance

You must always share personal data fairly and in a transparent manner.

- You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them.
- When you share personal data, you must ensure it is reasonable and proportionate. You must also ensure that the sharing happens in a way that people would not find unexpected or objectionable, unless there is a good reason.
- You must ensure that individuals know what is happening to their data. They must know which organisations are sharing their personal data and which ones have access to that information, unless an exemption or exception applies.
- Before sharing data, you must tell individuals about what you propose to do with their personal data in a way that is accessible and easy to understand.

In more detail

Fairness and transparency are central to the data processing principles in the GDPR. You must always process personal data fairly and in a transparent manner.

Fairness also forms a key part of the principles under the Law Enforcement provisions of Part 3 of the DPA. Transparency is provided for in section 44 of the DPA for Part 3 processing.

How do we comply with the fairness principle when sharing data?

This principle applies to general processing under the GDPR and to processing under Part 3 of the DPA.

- You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them.
- When you share personal data, you must ensure it is reasonable and proportionate.
- You must also ensure that the sharing happens in a way that people would not find unexpected or objectionable, unless there is a good reason. This is the case unless you are sharing due to a legal obligation or the sharing is necessary for law enforcement; the data sharing will take place despite any such concerns.
- You must comply with the fairness principle regardless of the type of sharing: whether you are sharing data on a routine basis or making a single one-off disclosure.
- You must meet the fairness requirement in data sharing in addition to demonstrating that you have a lawful basis for it. If any aspect of your processing is unfair, you will be in breach of the fairness principle – even if you can show that you have a lawful basis for the processing.
- You must treat fairly all the members of a group of individuals whose data you are sharing. If you treat most individuals fairly in your data sharing arrangement but treat even one individual unfairly, it will still be a breach of this principle.

Finally, sometimes data processing may take place in a way that negatively affects an individual but without this necessarily being unfair. The key here is whether the detriment is justified.

How do we assess whether we are sharing information fairly?

Some questions to consider:

- Is what you intend to do fair? Your planning process for the data sharing - including the steps as part of the DPIA (whether or not you are required to complete a DPIA) will help you to assess this.
- Should you share the personal data? Consider this, as well as thinking about how you can share the personal data.

- How did you obtain the data? For example, was anyone deceived or misled when you obtained the personal data? If so, using it for data sharing is unlikely to be fair.
- How does the data sharing affect the interests of the people whose data it is in general terms?

How do we comply with the transparency requirements when sharing data?

Individuals have to know what is happening to their data. The transparency principles under the GDPR and in section 44 in Part 3 of the DPA mean that you must ensure that individuals know which organisations are sharing their personal data and which ones have access to that information, unless an exemption or exception applies.

Before sharing data, you must tell individuals about what you propose to do with their personal data in a way that is accessible and easy to understand. You must use clear and plain language that is suitable for your audience.

What privacy information do we need to provide under the GDPR?

When you collect personal data from individuals, under Article 13 of the GDPR you must provide them with privacy information which sets out what you intend to do regarding the collection and use of their data, and who else will be involved, including recipients or categories of recipients. Doing this is part of your compliance with your transparency obligations, where appropriate, and also fairness.

When you collect personal data from a third party, under Article 14 you must provide that information to individuals within a reasonable period and at the latest within a month. In a data sharing context this could be controllers sharing and receiving the data. You must provide the individual with the information "at the latest" when you first disclose the data to another recipient.

There are different methods of providing privacy information to individuals. You can provide privacy information using one or more techniques, but you must:

- include certain specific content;
- keep it up to date and proactively issue new information if you change the purpose of your data sharing or commence new data sharing; and
- give the information directly to individuals.

For more details, please see the guidance on the ICO website at www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 5(1)(a), 13, 14 and Recitals 39, 58, 60-62 (external link)
See DPA 2018 Part 3 section 44 (external link)

Further reading outside this code of practice

ICO guidance on the right to be informed.
ICO guidance on the first principle

Security

At a glance

Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place. The security measures must be "appropriate" to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals. You must also take into account the state of the art and costs of implementation when determining what measures are appropriate for your circumstances.

In more detail

What does data protection law say about security?

Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place. The security measures must be "appropriate" to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

This chapter applies to processing under the GDPR and Part 3 of the DPA. These refer to security measures in relation to data processing in different ways:

- The security principle in the GDPR requires you to use "appropriate security"…"using appropriate technical or organisational measures ('integrity and confidentiality') and goes on to say more in Article 32.
- For Law Enforcement Processing under Part 3 of the DPA, you must use "appropriate technical or organisational measures" to ensure appropriate security of personal data.

You must also take into account the state of the art and costs of implementation when determining what measures are appropriate for your circumstances.

What are the security considerations when sharing data?

You should consider the following measures for information that you share with other organisations, or that they share with you:

- review the personal data that you receive from other organisations. Make sure you know its origin and whether any conditions are attached to its use;
- review the personal data that you share with other organisations. Make sure you know who has access to it and what they will use it for;
- make sure you provide a suitably high level of security when sharing special category or sensitive data;
- identify who within your organisation should have access to data that has been shared with you. Adopt "need to know" principles and avoid giving all your staff access to the data when only a few of them need it to carry out their job;
- consider the impact a personal data breach may have on individuals; and
- consider the impact a personal data breach could have on your organisation – in terms of cost, reputational damage or lack of trust from your customers or clients. For example, this can be particularly acute where individuals have provided you with their data, you share it with another organisation, and that recipient organisation fails to protect that data.

You should aim to build a culture of compliance and good practice throughout your organisation to help you to ensure you are sharing data securely. This must apply from Board level, through all employees and contractors. For example:

- it is essential that all your staff involved in data sharing understand the importance of protecting personal data; and
- you should check that the same applies across the organisations you are sharing data with.

Before sharing data, you should undertake an information risk analysis and document your conclusions. As part of the assessment, you should bear in mind the nature of the information you are sharing. For instance, is it special category or sensitive data? You should regularly test, assess and evaluate your security provision.

This must include the actual transmission of the data you are sharing, and the way the data will be handled afterwards. You should consider the measures that you need to put in place to secure the data.

However you must not forget all other aspects of security, both physical and technical. You need to ensure you know and regularly review your security measures, both physical and technical, in both your own office and, where appropriate, that of the organisation you are sharing the data with. Details matter, including who has access to the data, and what access controls are in place to all hardware and software. Remember to consider building and office security, and resilience in the case of an incident such as a power failure or a fire.

You should also have clear instructions about the security steps that need to be followed when sharing information by multiple methods, eg phone, fax, post, email, online or face to face.

Are we still responsible after we've shared the data?

Organisations that you share data with take on their own legal responsibilities for the data, including its security. However you should still take reasonable steps to ensure that the data you share will continue to be protected with adequate security by the recipient organisation:

- ensure that the recipient understands the nature and sensitivity of the information;
- take reasonable steps to be certain that security measures are in place, particularly to ensure that you have incorporated an agreed set of security standards into your data sharing agreement, where you have one; and
- you should resolve any difficulties before you share the personal data in cases where you and the recipient organisation have different standards of security, different IT systems and procedures, different protective marking systems etc.

Undertaking a DPIA for any data sharing operation can be an effective means of considering these issues and implementing appropriate mitigating measures.
You should also note that in certain circumstances you are required to do a DPIA when data sharing. Please refer to the section on DPIAs in the chapter on "Deciding to share data" in this code.

Relevant provisions in the legislation

See GDPR Articles 5(1)(f), 32, 35, and Recitals 39, 83 (external link)

See DPA sections 40 and 91

Further reading – ICO guidance

Read our guidance on security in the Guide to the GDPR for more information.

The ICO has also worked closely with the National Cyber Security Centre (NCSC) to develop a set of security outcomes that you can use to help determine what's appropriate for you. The security outcomes can also help you when considering any data sharing arrangements.

The rights of individuals

At a glance

In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights with ease. You should provide them with a single point of contact and have clear policies and procedures with the other organisations.
You must inform the other organisations about requests for erasure, rectification or the restriction of processing, unless it is impossible or disproportionate to do so.
There are additional requirements if your data sharing involves automated decision-making.
The position on individual rights is slightly different for Law Enforcement processing.

In more detail

What is the impact of the rights of individuals on data sharing?

In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights.

The rights available to an individual under the GDPR and under Part 3 of the DPA differ in some respects.

The GDPR gives individuals specific rights over their personal data. For general data processing under Part 2 of the DPA, in summary these are:

- the right to access personal data held about them (the right of subject access);
- the right to be informed about how and why their data is used - and you must give them privacy information;
- the rights to have their data rectified, erased or restricted;
- the right to object;
- the right to portability of their data; and
- the right not to be subject to a decision based solely on automated processing.

This chapter of the code does not seek to replicate existing ICO guidance on individual rights but rather focuses on how the rights impact on data sharing. You should refer to guidance on the ICO website www.ico.org.uk for more details.

How do you allow individuals to exercise their information rights in a data sharing scenario?

- You must have policies and procedures that allow individuals to exercise their rights with ease.
- If you are a joint controller these should be set out clearly in the transparent arrangement you and your other joint controller or controllers are required to enter into under Article 26 of the GDPR.
- You must provide details of how to exercise these rights in the privacy information you issue to individuals.

- You must make the exercise of individual rights as straightforward as possible. Be aware that although your DPO is responsible for being the first point of contact, individuals may contact any part of your organisation.
- Where several organisations are sharing data, it may be difficult for an individual to decide which organisation they should contact. You should make that clear in the privacy information you provide to them at the time you collect their data, as well as in any transparent arrangement made under Article 26.
- In a data sharing arrangement it is good practice to provide a single point of contact for individuals, which allows them to exercise their rights over the data that has been shared without making multiple requests to several organisations. However they are permitted to choose to exercise their rights against any controller they wish.

What is the impact on a data sharing arrangement of requests for erasure, rectification or the restriction of processing?

Under Articles 16, 17 and 18 of the GDPR, individuals have a right to request erasure, rectification of their data, or the restriction of processing of their data. As with other individual rights, you will make life easier for yourself and for the other organisations in a data sharing arrangement if you have clear policies and procedures about how to handle such requests.

Under Article 19 of the GDPR if you have shared information with other organisations you must inform them of the rectification, erasure or restriction of the personal data, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about those organisations.

How do we deal with complaints and queries from individuals about the sharing of their data?

From time to time individuals may have queries or complaints about the sharing of their personal data, particularly if they think the data is wrong or that the sharing is having an adverse effect on them.

The way you handle these queries and complaints makes a difference both to the individuals and to your organisation. It is not always a case of simply providing a response. The comments you receive might be an invaluable resource for you when you are reviewing your data sharing arrangement.

It is good practice to do the following:

- have procedures to deal with any complaints and queries in a quick and helpful way;
- provide a single point of contact;
- analyse the comments you receive in order to obtain a clearer understanding of public attitudes to the data sharing you carry out;
- take the opportunity to provide individuals with information about your data sharing further to that contained in your privacy information when answering their specific queries;
- if the responses you receive when you inform people about your data sharing consist of a significant number of objections, negative comments or other expressions of concern, use this information to help you review the data sharing in question;
- consider whether the comments you receive might suggest you should reduce the amount of data you share, or share it with fewer organisations;
- pay particular attention to concerns raised, and decide whether the sharing can go ahead in the face of public opposition. For example, you might decide to go ahead because you are under a legal obligation to share the data; and
- consider setting up focus groups to explore individuals' concerns, if you are carrying out large scale data sharing operations.

What do we need to do if the data sharing involves automated decision-making?

If your data sharing arrangement involves any automated decision-making, you must document the specific lawful basis for that automated decision-making in your data protection policy.

So individuals can exercise their rights, you must:

- provide them with information about the automated process and the risks it entails;
- send them a link to your privacy statement if you have obtained their personal data indirectly;
- explain how they can access details of the information you used to create their profile;
- tell those who provided you with their own personal data how they can object to profiling, including profiling for marketing purposes; and
- inform them, and have the relevant procedures in place, about their right to access the personal data input into the profiles so they can review and edit it for any accuracy issues.

In addition you must have checks for the profiling/automated decision-making systems in your data sharing, in order to protect any vulnerable groups (including children). You must ensure at all times that you only collect the minimum amount of data you need and have a clear retention policy for the profiles you create.

What do we need to do about solely automated processing subject to Article 22?

Article 22 of the GDPR gives individuals additional protective rights if your data sharing arrangement entails a solely automated decision-making process that has legal or similarly significant effects on them. For example, automated profiling, depending on the impact on individuals. You must carry out a DPIA where you assess under Article 35(3)(a) of the GDPR that your proposed data sharing, involving systematic and extensive profiling based on automated processing, will "produce legal effects concerning the natural person or will similarly affect the natural person".

You can only carry out this type of automated decision-making if the decision is:

- necessary for the entry into or performance of a contract with the individual;
- authorised by law (in this code, we are looking at specific UK legal provisions, eg for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

You must identify whether any elements of your data sharing arrangement fall under Article 22. If they do, you must:

- give information to individuals about the automated processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure that your systems are working as intended.

What individual rights are provided by Part 3 of the DPA: Law Enforcement Processing?

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

Certain rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. There are also exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights. There is more guidance on this on the ICO website at www.ico.org.uk

Example

A third sector organisation providing childcare services may hold information shared from a local authority and the NHS. The Article 26 transparency arrangement should set out a clear procedure that whichever organisation receives a request for personal data should take a lead on providing the data and notify the other parties if necessary.

The arrangement should also set out procedures for how to deal with the exercising of other individual rights.

The procedures should also be provided in privacy information and should also be contained in any data sharing agreement.

Relevant provisions in the legislation

See GDPR Articles 16-19 and 22
Part 3 of the DPA

Further reading outside this code of practice - ICO guidance

ICO guidance on the rights of data subjects
Individual rights under the Law Enforcement Processing provisions

Other legal requirements

At a glance

In addition to identifying a lawful basis for your data sharing, you must ensure that your data sharing is lawful in a more general sense in order to comply with the lawfulness principle.

For public sector bodies this includes identifying whether you have a legal power to share data.

Most private and third sector organisations do not need to identify a specific power to share data. They have a general ability to share information, provided this does not breach the data protection legislation or any other law. If you are a private sector organisation you should check your constitutional documents, legal agreements or any other legal or regulatory requirements to make sure there are no restrictions that would prevent you from sharing personal data in a particular context.

In more detail

The code has considered the data sharing requirements of the data protection legislation. This chapter now looks at some other requirements. It discusses the legal constraints on you, outside data protection legislation, and the legal powers you have to share data.

Before sharing any personal data, you must consider all the legal implications of doing so. In addition to identifying a lawful basis for your data sharing, you must ensure that your data sharing is lawful in a more general sense in order

to comply with the lawfulness principle. For public sector bodies this includes identifying whether you have a legal power to share data.

You must not confuse the lawfulness principle with legal powers. There is a link, though - if you do not have the legal power to share data, you will be in breach of the lawfulness principle.

Do we have a legal power to share data?

If you wish to share information with another organisation, either by way of a one-off disclosure or as part of a routine data sharing arrangement, you need to consider:

- whether you have a general legal power to share information, for instance, under your constitution. This is likely to be more relevant to public sector organisations; and
- what type of organisation you are, because your legal status also affects your ability to share information, in particular, it depends on whether you are within the public, private or third sector.

What are the legal powers in the public sector?

When deciding whether you may proceed with any data sharing initiative, you should identify the legislation that is relevant to you. Even if this does not mention data sharing explicitly - and usually it will not do so - it is likely to lead you to a clearer understanding of your legal position.

Most public sector organisations derive their powers entirely from statute - either from the Act of Parliament which set them up, or from other legislation regulating their activities. The exceptions are government departments headed by a Minister of the Crown (which have common law powers to share information).

The relevant legislation will probably define your functions in terms of your purposes, the things that you must do, and the powers you may exercise in order to achieve those purposes. So you should identify where the data sharing in question would fit, if at all, into the range of things that you are able to do. Broadly speaking, there are three ways in which you may do so:

- **Express statutory obligations**

Occasionally, a public body will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances.

- **Express statutory powers**
  Sometimes, a public body will have an express power to share information. An express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways". For instance, specific gateways exist under the Digital Economy Act 2017 (the DEA). Under the DEA there is a framework providing a legal gateway for data sharing for defined purposes between specified public authorities, for the public benefit. Please see elsewhere in this code for more details.

- **Implied statutory powers**
  Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. Public authorities are likely to rely on the public task lawful basis in Article 6(3) of the GDPR. This requires the power to be laid down by law - but this does not need to be an explicit statutory provision. You can rely on this power to share data so long as it is sufficiently foreseeable and transparent.

Whatever the source of your power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question. If it does not, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place.

What are the legal powers for private and third sector organisations?

The legal framework that applies to private and third sector organisations differs from that for public sector organisations. Most private and third sector organisations do not need to identify a specific power to share data. They have a general ability to share information, provided this does not breach the data protection legislation or any other law. If you are a private sector organisation you should check your constitutional documents, legal agreements or any other legal or regulatory requirements to make sure there are no restrictions that would prevent you from sharing personal data in a particular context. Big organisations with complex, larger scale processing should consider obtaining legal advice.

Private and third sector organisations should pay attention to any industry-specific regulation or guidance about handling personal data, as this might affect your ability to share information.

What is the impact of human rights law?

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector in so far as they carry out functions of a public nature.

Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights (the Convention). Article 8 of the Convention, which gives everyone the right to respect for their private and family life, home and correspondence, is especially relevant to the sharing of personal data.

If you disclose or share personal data only in ways that comply with the data protection legislation, the sharing or disclosure of that information is also likely to comply with the HRA.

You should seek specialist advice if you have any concerns about human rights issues, other than the data protection elements of Article 8, about the disclosure or data sharing arrangement you are proposing.

Have you checked whether there are any legal prohibitions on data sharing?

Your ability to share information may be subject to a number of legal constraints outside the data protection legislation. There might be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that might affect your ability to share personal data.
A duty of confidence might be stated explicitly, or it might be implied, either by the content of the information or because it was collected in circumstances where confidentiality is expected, eg medical or banking information. If you are a big organisation planning to carry out complex, larger scale processing, you should consider obtaining legal advice on your data sharing plans.

In some private sector contexts there are legal constraints on the disclosure of personal data, other than data protection legislation.

Relevant provisions in the legislation

European Convention on Human Rights: Article 8

Further reading outside this code

Lawful basis for processing
Guide to Law Enforcement Processing

Law Enforcement Processing: Part 3 DPA

At a glance

Most data sharing, and hence the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a "competent authority" for specific law enforcement purposes is subject to a different regime under Part 3 of the DPA for Law Enforcement Processing, which provides a separate but complementary framework. As a competent authority, it is very likely that you will also be processing personal data for general purposes under Part 2 of the DPA, eg for HR-related matters. In that instance, you should follow the general guidance for Part 2 / GDPR data sharing.

In more detail

There are often compelling reasons why data sharing is needed for law enforcement purposes. We are aware that sometimes, organisations are hesitant about data sharing in this context. However, we emphasise that data protection legislation does not prevent appropriate data sharing when it is necessary to protect the public, to support ongoing community policing activities, or in an emergency for example. Adhering to the provisions of the legislation and following the good practice set out in this code will help you to share data in a compliant and proportionate way.

Example

Requests for information made by competent authorities must be reasonable in the context of their law enforcement purpose, and the necessity for the request should be clearly explained to the organisation.

For example, the police might ask a social worker to pass on case files to police containing details of young teenagers.

The social worker might feel reluctant to voluntarily disclose information to the police if the request appears excessive, or the necessity or urgency appears unjustified. The police should provide as much clarity as they can, without prejudicing their investigation.

Most data sharing, and hence the bulk of this code, is covered by the general processing provisions under Part 2 of the DPA; in practice this means referring to the GDPR. However data sharing by a **competent authority** for specific **law enforcement purposes** is subject to a different regime under Part 3 of the DPA, which provides a separate but complementary framework.

What is a competent authority?

A competent authority means:

- a person specified in Schedule 7 of the DPA; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes (section 30(1)(b) of the DPA 2018).

You need to check whether you are listed as a competent authority in Schedule 7 of the DPA. The list includes most government departments, police chief constables, the Commissioners of HMRC, the Parole Boards and HM Land Registry.

If you are not listed in Schedule 7, you may still be a competent authority if you have a legal power to process personal data for law enforcement purposes. For example, local authorities who prosecute trading standards offences or the Environment Agency when prosecuting environmental offences.

What are the law enforcement purposes?

This term is defined in section 31 of the DPA as:

Quote

"the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

Law enforcement must be the primary purpose of the processing.

Even if you are a competent authority, it is very likely that you will also be processing personal data for general purposes under Part 2 of the DPA, rather than for law enforcement purposes. An example might be for HR-related matters. In that instance, you should follow the general data sharing guidance contained elsewhere in this code.

We are a competent authority: how do we share data?

If you are a competent authority, and the sharing is for law enforcement purposes, then Part 3 may provide a framework allowing you to share data.

This differs in some ways from the provisions in Part 2 and the GDPR. The differences include lawful basis, and are primarily because of the purpose for which you are processing the data.

In particular, there are only six principles in Part 3, and processing of data described in Part 3 as "sensitive" is subject to additional safeguards, such as conditions in Schedule 8 of the DPA.

How do we share data with a competent authority?

If you are an organisation that **does not** fall within the Part 3 definition of a competent authority, then you can still share data for law enforcement purposes with a competent authority, such as the police in compliance with the GDPR. However you must still have a lawful basis for the sharing and you are also likely to need a condition for disclosing the data under Schedule 1 of the DPA.

Requests for information made by competent authorities must be reasonable in the context of their law enforcement purpose, and they should clearly explain the necessity for the request to you.

Where necessary in the circumstances, you can also rely on the "crime and taxation" exemption in DPA schedule 2, paragraph 2(1) from some GDPR provisions. This includes transparency obligations and most individuals' rights, if the application of these provisions is likely to prejudice the prevention or detection of crime.

If you are not a competent authority and are disclosing data relating to criminal offences and convictions (including allegations) you must comply with Article 10 of the GDPR. In practice this means:

- you again need to meet a relevant condition in Schedule 1 of the DPA 2018. In this scenario, the most likely condition is in Schedule 1 paragraph 10: disclosures necessary for prevention or detection of unlawful acts; and
- if meeting the public interest requirement is a problem, paragraph 36 of Schedule 1 provides a fall-back condition permitting the disclosure of criminal offence data, providing that the disclosure is necessary for the purposes of preventing or detecting an unlawful act; and asking for the individual's consent would prejudice those purposes.

If the data you are sharing includes special category data (eg information about race, ethnic origin, religion or biometric data), a condition under Article 9 of the GDPR will need to apply together with a linked condition in Schedule 1 of the DPA in most cases (most likely Article 9(2)(g) together with Schedule 1 paragraph 10 of the DPA).You must be able to demonstrate that the data sharing is necessary for reasons of substantial public interest.

The DPA usually requires organisations to have an "appropriate policy document" to cover their processing under this condition. However, an organisation disclosing data to a competent authority does **not** need to have a policy document to cover that disclosure.

Example

A shopkeeper used CCTV, and routinely captured footage of customers in the premises. A copy of some CCTV footage was requested by a police force for an ongoing criminal investigation. The police force told the shopkeeper why it wanted it (some competent authorities may use a standard form for this).

The shopkeeper was processing data under the GDPR. Assuming the shopkeeper had a lawful basis for the processing, she could rely on Schedule 1, paragraph 10 to process the CCTV data, and give the police a copy of the footage to help with the investigation.

The receiving police force (competent authority) was processing the information under Part 3 of the DPA 2018. This helped it to fulfil its statutory functions.

How do we allow individuals to exercise their information rights in a data sharing scenario under Part 3?

There are differences in the availability of individual rights for law enforcement processing. Certain individual rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the DPA. There are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights if there is a likely prejudice to the law enforcement purposes.

For further details on this, please refer to the ICO guidance on law enforcement processing at www.ico.org.uk.

How do we comply with the accountability requirement under Part 3?

Part 3 of the DPA requires you, as controller, to demonstrate that you comply with the principles. You are accountable.

You must put in place appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include policies and procedures, including data protection by design and default.

Example

There is an example earlier in the code, in the chapter on accountability, about the inappropriate disclosure of unredacted information by a council from a police intelligence database on gangs.

The police's own use of the gangs database in such an example would also need to address key issues of data retention, security, excessive data collection and sharing to enable the gangs programme to be lawful.
The aim of the data sharing between police and public sector organisations such as the local council to counter gang culture is a valid public interest to pursue.

A fair approach to data sharing, which is transparent in its purpose and accountable to obligations under data protection law, will gain the trust of our communities that are most directly affected, and so enhance the ability of community policing to engage with them.

You must also maintain relevant documentation of data processing activities. For more details, please refer to the ICO guidance on Law Enforcement Processing.

We have set out below the particular requirements of Part 3 documentation for data sharing.

Categories

When sharing data for law enforcement purposes, where relevant and as far as possible, you must make a clear distinction between different categories of personal data. You must distinguish between people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;

- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

Internal records of processing activities

Under Part 3 you must maintain detailed records of all data processing activities you undertake. This is a legal obligation. Your records must include the sort of details you would expect, such as:

- the purposes of your processing (this obviously includes any data sharing arrangements);
- categories of organisations with which you share personal data;
- the name of your DPO; and
- your security measures.

Logging

The following is likely to apply to many competent authorities that carry out data sharing. If your organisation operates any IT database for data processing, under Part 3 you must keep logs for specific processing operations such as collection, alteration, erasure and disclosures (including transfers). For more details, please refer to the ICO guidance on Law Enforcement Processing.

Relevant provisions in the legislation

See GDPR Articles 6, 9, 10 and Recitals 40, 41, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56 (external link)

See DPA 2018 sections 10, 11(2), 15, 30(1)(b), 31 and schedule 1 (paragraphs 10 and 36), 2 (paragraph 2) and 7 (external link)

Further reading outside this code of practice

Guide to Law Enforcement Processing
Guide to data protection

Due diligence when sharing data following mergers and acquisitions

At a glance

If merger or acquisition or other change in organisational structure means that you have to transfer data to a different or additional controller, you must take care. You must ensure you consider data sharing as part of the due diligence you carry out, including establishing the purposes for which the data was originally obtained, and your lawful basis for sharing it. You must comply with the principles, and document your data sharing. Consider when and how you will inform individuals about what's happening to their data. You must also ensure sound governance, accountability and security.

In more detail

This chapter is of particular relevance to the private sector. It highlights situations such as mergers and acquisitions, or other changes in organisational structure, where you need to make good data sharing practice a priority.

How does data sharing apply to mergers and acquisitions?

Data sharing considerations may become a priority when a merger or acquisition or other change in organisational structure means that you have to transfer data to a different organisation. For example, as part of a takeover, data might be sold as an asset to a different legal personality. You must take care if, as a result of the changes, there is a change in the controller of the data, or if the data is being shared with an additional controller. This is the case whether you are the sharing or recipient controller. We will look at this from the point of view of the organisation sharing the data with a different controller:

- ensure that you consider the data sharing as part of the due diligence you carry out;
- follow the data sharing guidance contained in this code;
- establish what data you are transferring;
- identify the purposes for which the data was originally obtained;
- establish your lawful basis for sharing the data;
- ensure you comply with the data processing principles - especially lawfulness, fairness and transparency to start with;
- document the data sharing;
- seek technical advice before sharing data where different systems are involved: there is a potential security risk that could result in the loss, corruption or degradation of the data; and
- consider when and how you will inform individuals about what is happening. Under the GDPR you are required to keep individual data subjects informed about certain changes relating to the processing of their data, and they may have a right to object. Please see the guidance on individual rights on the ICO website at www.ico.org.uk.

The same considerations may apply in reverse to the controller receiving the data.

How do we manage shared data following a merger or restructure or other change of controller?

On a practical level, it can be difficult to manage shared data immediately after a change of this kind, especially if you are using different databases, or you are trying to integrate different systems. It is particularly important in this period to consider the governance and accountability requirements of the GDPR. You must:

- check that the data records are accurate and up to date;
- ensure you document everything you do with the data;
- adhere to a consistent retention policy for all records; and
- ensure appropriate security is in place.

Relevant provisions in the legislation

See GDPR Articles 5, 6, 7 and 21 and Recitals 39, 40, 42, 43, 50, 69, 70

Further reading outside this code

Guidance on individual rights under the GDPR

Sharing personal data in databases and lists

At a glance

The transfer of databases or lists of individuals, whether for money or other consideration, and whether for profit or not, is a form of data sharing. This may include sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies, and political parties.

It is your responsibility to satisfy yourself about the integrity of the data supplied to you. You are responsible for compliance with the law for the data you receive, and you will have to respond to any complaints about it. You should make appropriate enquiries and checks, including:

- confirm the source of the data;
- identify the lawful basis on which it was obtained;
- check what individuals were told at the time of handing over their data;
- verify details of how and when the data was initially collected;
- check the records of consent, if relevant;
- review a copy of the privacy information given at the time of collection of the data;
- check what information was given to individuals in accordance with Article 14 of the GDPR - ie privacy information that must be given when data is obtained from a source other than the data subject;
- check that the data is accurate and up to date; and
- ensure that the data you receive is not excessive or irrelevant for your needs.

In more detail

How does data sharing apply to the acquisition or transfer of databases and lists?

The transfer of databases or lists of individuals, whether for money or other consideration, and whether for profit or not, is a form of data sharing. This chapter considers data sharing which has not resulted from organisational changes.

Examples of organisations involved in this type of data sharing may include:

- data brokers;
- credit reference agencies;
- marketing agencies;
- franchised businesses;
- individual parts of a business that operate independently from their head office;
- clubs and societies;
- charities; and
- political parties.

The data protection legislation allows you to do this, so long as you comply with the law. You will also find it beneficial to follow the good practice set out in this code. The due diligence carried out by both the sharing and recipient controller is crucial to compliance.

We will look at this from the viewpoint of the organisation receiving the database or list. The organisation sharing the data should follow a similar process.

What must we do to ensure the database or list we are receiving is being shared in compliance with the law?

It is your responsibility to satisfy yourself about the integrity of the data supplied to you. You are responsible for compliance with the law for the data

you receive, and you will have to respond to any complaints about it. You should make appropriate enquiries and checks, including the following:

- confirm the source of the data;
- identify the lawful basis on which it was obtained;
- check what individuals were told at the time of handing over their data;
- verify details of how and when the data was initially collected;
- check the records of consent, if relevant;
- review a copy of the privacy information given at the time of collection of the data;
- check what information was given to individuals in accordance with Article 14 of the GDPR - ie privacy information that must be given when data is obtained from a source other than the data subject;
- check that the data is accurate and up to date; and
- ensure that the data you receive is not excessive or irrelevant for your needs.

You should consider having a written contract with the organisation supplying you with the data.

What else do we need to do?

Under Article 14 of the GDPR you must give privacy information to individuals whose data has been shared with you "…within a reasonable period after obtaining the personal data, but at the latest within one month…".

How does data sharing interact with direct marketing?

If this form of data sharing is relevant to your data sharing arrangement you should read the ICO's detailed guidance on direct marketing. We will be issuing an updated direct marketing code of practice; you should refer to the ICO website at www.ico.org.uk.

How does data sharing interact with political campaigning?

Political parties, referendum campaigners and candidates use information about voters to help to target their campaign materials more effectively; they may:

- buy lists and databases from organisations such as data brokers; and
- use third parties to send out campaign materials.

This involves data sharing; and communicating with voters, such as via social media platforms and targeting political messages, may amount to direct marketing.

You should carry out the checks described earlier in this chapter in order to satisfy yourself about the integrity of the data supplied to you.

If you use a third party organisation to send out campaign materials on your behalf using your database, you are sharing data with that external organisation. You should apply diligence in checking and monitoring what the third party is doing. You are responsible as controller for that data and for compliance with the legislation. You should read and follow the ICO guidance on the law relating to political campaigning and direct marketing on the website at www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 13 and 14

Further reading outside the code of practice – ICO guidance

See the Direct marketing code and guidance on the ICO website in due course www.ico.org.uk

See the new Political campaigning guidance soon to be published on the ICO website www.ico.org.uk

See the Guide to Privacy and Electronic Communications Regulations (PECR)

Data sharing and children

At a glance

If you are considering sharing children's personal data, you must proceed with caution. You must consider the best interests of the child. You should consider the need to protect them from the outset.

You should build this into the systems and processes in your data sharing arrangement. A high level of privacy should be your default.

We recommend that you do a DPIA to assess the risks involved in sharing this data. Sharing children's data with third parties can expose them to risks. If the data sharing is of a type likely to result in a high risk to children's rights and freedoms, a DPIA is compulsory.

In more detail

- What do we need to bear in mind when sharing children's data?

What do we need to bear in mind when sharing children's data?

- You need to consider the best interests of the child. This concept comes from the United Nations Convention on the Rights of the Child (UNCRC), which declares that "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." In essence, the best interests of the child are whatever is best for that individual child.
- You have to balance the best interests of the child against the rights of others. For example, it is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy.
- Considering the best interests of the child should form part of your compliance with the lawfulness, fairness and transparency principle.

- Fairness, and compliance with the data protection principles, should be central to all the sharing you carry out of children's personal data. Is it fair to share the child's data? What is the purpose of the sharing?
- Children are less aware than adults of the risks involved in having their data collected and processed, so you have a responsibility to assess the risks and put appropriate measures in place. Where appropriate, consider children's views when designing your data sharing arrangement.
- The privacy information you provide must be clear and presented in plain, age-appropriate language.
- You should carry out due diligence checks on the organisations with which you are planning to share data. You should consider what the organisation you are sharing the data with plans to do with it. If you can reasonably foresee that the data will be used in a way that is detrimental to the child, or otherwise unfair, then you shouldn't share.
- You should ensure that any default settings relating to data sharing specify the purpose of the sharing and who the data will be shared with. Settings which allow general or unlimited sharing will not be compliant.
- You should not share personal data unless you have a compelling reason to do so, taking account of the best interests of the child. One clear example of a compelling reason is data sharing for safeguarding purposes. Whereas selling on children's personal data for commercial re-use is unlikely to amount to a compelling reason for data sharing.
- Consent is not the only lawful basis to use. Other lawful bases might be more appropriate.
    - If you are relying on consent, you must consider the competence of the child to give their own consent, and whether that consent is freely given (eg where there is an imbalance of power).
    - You should also consider the child's competence if you are relying on the lawful basis that the sharing is necessary for the performance of a contract.
- If you (or another data controller in the data sharing arrangement) are a provider of an online service then you also need to comply with the Age-appropriate design code.

There is more information on all the above on the ICO website www.ico.org.uk

Relevant provisions in the legislation

See GDPR Articles 6(1), 8, 12(1) and Recitals 38, 58, 65, 71, 75

Further reading outside the code of practice

Guide to data protection: children
Children and the GDPR

United Nations Convention on the Rights of the Child

Data sharing in an urgent situation or in an emergency

At a glance

In an emergency you should go ahead and share data as is necessary and proportionate. If you are likely to be involved in responding to emergency situations it will be helpful to plan ahead as far as possible, by considering the types of data you hold and which data you are likely to need to share in advance.

In more detail

Much of the guidance in this code envisages that you are carrying out data sharing on a routine basis and that you have the opportunity and time to plan carefully ahead. However this might not always be the case.

What should we do in an emergency?

Urgent or emergency situations can arise that you may not have envisaged, and have to be dealt with on the spot. In an emergency you should go ahead and share data as is necessary and proportionate.

Tragedies over recent years such as the Grenfell Tower fire, and major terrorist attacks in London and Manchester, have illustrated the need for joined-up public services where data sharing can make a real difference to public safety. In these situations it would be more harmful not to share the data than to share it. You should factor in the risks involved in not sharing data.

How can we plan ahead for data sharing in urgent situations?

In an emergency situation, you have to take decisions rapidly. Often, forward planning will help. Emergency services plan for various scenarios, and in the same way you should plan ahead for your organisation. In urgent or emergency situations, where there is less time to consider issues in detail, it can be particularly difficult to make sound judgements about whether to share information.

Likewise, there can be reasons why organisations and agencies are hesitant to share information during both the planning and recovery phases, where the need to share information may not be as urgent.

The key point is that the DPA does not prevent organisations sharing personal data where it is appropriate to do so. Factoring in the risks involved in not sharing data is particularly relevant in this situation.

Where possible, if you are likely to be involved in responding to emergency situations you should consider the types of data you are likely to need to share in advance. As part of this it would be useful to consider any pre-existing DPIA. All this should help you to establish what relevant data you hold, and help to prevent any delays in an emergency.

All types of organisations might have to face an urgent but foreseeable situation, so you should have procedures about the personal data you hold and whether, and how, you should share any of this information.

Example

The police, the fire service and local councils get together to plan for identifying and assisting vulnerable people in their area in an emergency situation such as a flood, a major fire or a terrorist incident. As part of the process they determine what type of personal data they each hold and have a data sharing agreement to set out what they will share and how they will share it in the event of an emergency.

They review this plan at regular scheduled intervals.

Data sharing across the public sector: the Digital Economy Act codes

At a glance

The government has devised a framework for the sharing of personal data, for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (the DEA). The aim is to improve public services through the better use of data, while ensuring privacy, and to ensure clarity and consistency in how the public sector shares data. The DEA codes, which are required to be consistent with this data sharing code, provide guidance on the proportionate exercise of the tightly-defined DEA data sharing powers, in compliance with the data protection legislation.

The government introduced a framework for the sharing of personal data for defined purposes across specific parts of the public sector, under the Digital Economy Act 2017 (the DEA): the DEA framework. (Note that the DEA framework is distinct from the Framework for Data Processing by Government in section 191 of the DPA).

Its aim is to ensure clarity and consistency in how the public sector shares personal data, improving public services through the better use of data, while ensuring data privacy. The government also made it clear that data should only be shared when there is a clear public benefit.

Part 5 of the DEA focuses on Digital Government, providing gateways that allow specified public authorities to share personal data with each other, in order to improve the delivery of public services. The objectives and purposes for data sharing under the DEA powers are tightly defined.

The organisations must still comply with the data protection legislation.

Part 5 of the DEA explicitly:

- states that all processing of information under the DEA powers must be in compliance with the data protection legislation; and
- prohibits the disclosure of information where it would contravene the data protection legislation.

Note that whilst the DEA predates the GDPR, it was drafted with a view to being consistent with GDPR provisions.

The powers to share information under Part 5 of the DEA are supplemented by statutory codes of practice (the DEA codes) which must be consistent with the Information Commissioner's data sharing code of practice "as altered or replaced from time". The codes must follow the data protection principles, ensuring that the sharing of personal data under the DEA powers is proportionate.

For example, there is a DEA code for public authorities sharing personal data information about the following aspects of public service delivery to:

- achieve specified public service delivery objectives;
- assist people living in fuel poverty and water poverty; and
- manage debt and fraud against the public sector.

There are also provisions in the DEA facilitating data sharing by and with the Statistics Board to allow the production of statistics, disclosure of information by civil registration officials, and data sharing for research purposes.

The DEA codes contain guidance as to what data you can share and for which purpose. They include safeguards to make sure that the privacy of citizens' data is protected. Public authorities have to put in place a data sharing agreement, described in the DEA codes as an "information sharing agreement".

Anyone who discloses information under the DEA Part 5 powers must also "have regard" to other codes of practice issued by the Information Commissioner "so far as they apply to the information in question":

- on the identification and reduction of risks to privacy of a proposal to disclose information; and
- the information to be provided to individuals about the use to be made of information collected from them.

More information will follow on the ICO website www.ico.org.uk about the DEA data sharing framework.

Relevant provisions in the legislation

Digital Economy Act 2017

Further reading outside this code

Digital Economy Act Part 5 Codes of practice

Data ethics and data trusts

At a glance

You should bear in mind ethical factors in addition to legal and technical considerations when deciding whether to share personal data.

Data trusts are a relatively recent concept: a legal structure that enables independent third-party stewardship of data. Pilot projects have taken place to demonstrate their use in data sharing.

In more detail

What is a data trust?

There is a great deal of interest, both in the UK and internationally, in the concept of 'data trusts'. There are various definitions of data trusts. The Open Data Institute (ODI) defines them as "a legal structure that provides independent third-party stewardship of data". In essence they are a new model to enable access to data by new technologies (such as artificial intelligence), while protecting other interests and retaining trust, and following a "privacy by design" approach. They have potential for use in data sharing.

What has been happening in the area of data trusts?

In 2019 the UK government announced that the ODI would be working with others on pilot projects to examine how a data trust could increase access to

data while retaining trust. It was also announced that in due course the ODI would make proposals as to the future use of data trusts.

The ICO will publish more information on data trusts in the future; please see the ICO website at www.ico.org.uk.

Is it ethical to share this data?

When deciding whether to enter into a data sharing arrangement, you should consider how that sharing would affect the individual's information rights, from an ethical stance.

Ask yourself whether it is:

- right to share that data in that particular way;
- the action of a responsible organisation;
- properly justified; and
- subject to clear and strong safeguards?

Data protection principles are based on respect for the fundamental rights of individuals. This is reflected in the requirements of the data protection legislation for fairness, transparency and accountability when processing personal data. Broadly speaking, ethical principles form a part of considerations on proportionality and fairness and are complementary to data protection principles. You should consider them in addition to considering the lawfulness and the technical requirements of data sharing.

What else should we consider?

You should also consider:

- any imbalance of power. There is a significant imbalance of power between organisations and individuals, and in particular vulnerable individuals. As an organisation you should act responsibly towards the needs not only of wider society but also of the individual; and
- the impact the data sharing would have on individuals' information rights regarding issues such as social exclusion, as well as on matters of equality and fundamental human rights. These might be the very matters you are intending to help to address in your data sharing plans,

so you need to give this careful thought, as you might need to strike a delicate balance.

What has been happening in the area of data ethics?

The UK government has taken an interest in data ethics.

In 2017 it announced the establishment of the Centre for Data Ethics and Innovation (CDEI) to investigate and advise on the use of data and data-enabled technologies and artificial intelligence, both in the public and private sectors.

In 2018 it published a Data Ethics Framework setting out clear standards for how data should be used in the public sector, with the aim of building confidence in public sector data use.

In 2015, the UK Statistics Authority (UKSA) established the National Statistician's Data Ethics Advisory Committee to provide independent and transparent advice to the National Statistician that the collection, access, use and sharing of data, for research and statistical purposes, is ethical and for the public good. The UKSA has also developed a self-assessment toolkit to provide guidance and support to researchers on how to assess and mitigate ethical risks in the context of their research.

Further reading outside this code of practice

Open Data Institute website
ODI article on data trusts
Government data ethics framework
Centre for Data Ethics and Innovation website
The National Statistician's Data Ethics Advisory Committee

Enforcement of this code

At a glance

The ICO upholds information rights in the public interest. In the context of data sharing, our focus is to help you carry out data sharing in a compliant way.

We have various powers to take action for a breach of the GDPR or DPA where appropriate. This includes the power to issue warnings, reprimands, stop-now orders and fines. We will always use our powers in a targeted and proportionate manner, in line with our regulatory action policy.

In more detail

What is the role of the ICO?

The Information Commissioner is the independent supervisory authority for data protection in the UK.

Our mission is to uphold information rights for the public in the digital age. Our vision for data protection is to increase the confidence that the public have in organisations that process personal data. We offer advice and guidance, promote good practice, monitor and investigate breach reports, monitor compliance, conduct audits and advisory visits, consider complaints, and take enforcement action where appropriate. Our enforcement powers are set out in part 6 of the DPA.

We have also introduced initiatives such as the Sandbox to help support organisations using personal data to develop innovative products and services.

Where the provisions of this code overlap with other regulators we will work with them to ensure a consistent and co-ordinated response.

How will the ICO monitor compliance?

We will use this code in our work to assess the compliance of controllers through our audit programme and other activities.

Our approach is to encourage compliance. Where we do find issues we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected.

How does the ICO deal with complaints?

If someone raises a concern with us about your data sharing, we will record and consider their complaint.

We will take this code into account when considering whether you have complied with the GDPR or DPA, particularly when considering questions of fairness, lawfulness, transparency and accountability.

We will assess your initial response to the complaint, and we may contact you to ask some questions and give you a further opportunity to explain your position. We may also ask for details of your policies and procedures, your DPIA, and other relevant documentation. However, we expect you to be accountable for how you meet your obligations under the legislation, so you should make sure that when you initially respond to complaints from individuals you do so with a full and detailed explanation about how you use their personal data and how you comply.

If we consider that you have failed (or are failing) to comply with the GDPR or DPA, we have the power to take enforcement action. This may require you to take steps to bring your operations into compliance or we may decide to fine you or both.

What are the ICO's enforcement powers?

We have various powers to take action for a breach of the GDPR or DPA. We have a statutory duty to take the provisions of this code into account when enforcing the GDPR and DPA.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to €20 million or 4% of your annual worldwide turnover, whichever is higher.

In line with our regulatory action policy, we take a risk-based approach to enforcement. Our aim is to create an environment within which, on the one hand, data subjects are protected, while ensuring that business is able to operate and innovate efficiently in the digital age. We will be as robust as we need to be in upholding the law, whilst ensuring that commercial enterprise is not constrained by red tape, or concern that sanctions will be used disproportionately.

These powers are set out in detail on the ICO website at www.ico.org.uk.

Relevant provisions in the legislation

See GDPR Articles 12-22 and Recitals 58-72 (external link)
See DPA 2018 section 129-164 and schedule 12 (external link)

Further reading outside this code

What we do
Make a complaint
Regulatory Action Policy
Guide to the ICO Sandbox - beta phase

Annex A: data sharing checklists

These will be added before the final publication stage.

Annex B: template data sharing request and decision forms

These will be added before the final publication stage.

Annex C: data protection principles

The data protection principles for the general processing of data (ie under part 2 of the DPA) are those stated in the GDPR. However there are some differences in the principles applicable to Law Enforcement Processing under Part 3 and Intelligence Services Processing under Part 4.

For your ease of reference, we have reproduced each of them below. You should also refer to the ICO's guidance at www.ico.org.uk

- GDPR data protection principles
- Data Protection Act 2018 Part 3: Principles applicable to Law Enforcement Processing

GDPR data protection principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data

are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Data Protection Act 2018 Part 3: Principles applicable to Law Enforcement Processing

34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

35 The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(6) The Secretary of State may by regulations amend Schedule 8—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8) In this section, "sensitive processing" means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

36 The second data protection principle

(1) The second data protection principle is that—

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—

(a) the controller is authorised by law to process the data for the other purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

37 The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

38 The fourth data protection principle

(1) The fourth data protection principle is that—

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—

(a) persons suspected of having committed or being about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) persons who are or may be victims of a criminal offence;

(d) witnesses or other persons with information about offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose—

(a) the quality of personal data must be verified before it is transmitted or made available,

(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

39 The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

40 The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Annex D: case studies

Fairness and transparency

Supermarket providing privacy information to customers

A supermarket holds information about its customers through its 'loyalty' card scheme, in-store CCTV and records of payments. The company does not normally disclose any information to third parties, for example for marketing purposes. However, it would do so if the information it held were relevant to a police investigation or in response to a court order, for example.

The supermarket or the card scheme operator should have given customers privacy information that provided an explanation, in general terms, of the sorts of circumstances in which it would share information about scheme members with a third party, such as the police.

If the supermarket discloses information about a particular scheme member to the police, it does not need to inform the individual of the disclosure if this would prejudice crime prevention.

Fairness and transparency

Sharing customer details with a credit reference agency

A mobile phone company intends to share details of customer accounts with a credit reference agency.

It must inform customers when they open an account that it will share information with credit reference agencies.

Credit reference agencies need to be able to link records to the correct individual, so the mobile phone company must ensure it is collecting adequate information to distinguish between individuals, for example dates of birth.

The organisations involved must have procedures to deal with complaints about the accuracy of the information they have shared.

Fairness and transparency; privacy information

Public sector bodies sharing data to provide a co-ordinated approach

Personal information is shared between two county councils and 19 relevant partner organisations in order to prevent social exclusion amongst young people who have been, or are at high risk of disengaging from education, employment or training. By sharing information the partner organisations can ensure a co-ordinated approach to identifying and contacting each young person to offer the most appropriate support to encourage them back in to education, work or training.

As part of developing their data sharing agreement, all the partners updated their privacy notices to include this new data sharing and agreed that each organisation would communicate this via their websites as well as in correspondence and conversations their staff have with the young people.

Fairness and transparency

Duty to process data fairly when carrying out research using shared data

A local university wants to conduct research into the academic performance of children from deprived family backgrounds in the local area. The university wants to identify the relevant children by finding out which ones are eligible for Pupil Premium. Therefore it decides to ask all local primary and secondary schools to share this personal data, as well as the relevant children's test results for the past three years.

The DPA contains various provisions that are intended to facilitate the processing of personal data for research purposes. However, there is no exemption from the general duty to process the data fairly. Data about families' income levels, or eligibility for benefits, may be inferred from the Pupil Premium status of a child. Parents and their children may well object to the disclosure of this data because they consider it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.

Instead the school could identify eligible children on the researchers' behalf and contact their parents, explaining what the research is about, what data the researchers want. The school might wish to obtain parents' consent for the sharing of the data, but other lawful bases would be available to it.

Alternatively, the school could disclose an anonymous data set, or statistical information, to the researchers.

Data sharing agreement; accountability

Information sharing framework in healthcare

Healthcare partners in one county decided to develop an information sharing framework to standardise their sharing processes and encourage agencies to share personal data safely. The framework helped their staff to comply with data protection legislation by sharing information lawfully, securely and confidentially. As a result they were able to integrate service provision across the county and deliver better care outcomes for their residents. In a key step, partners brought together information governance leads to oversee the changes needed to develop the framework.

Main purposes of the framework were to ensure that:

- people only have to tell their story once and can expect a better service delivery;
- local people have clear guidance about how their information is shared (and in what circumstances their consent may need to be sought to share it);
- professionals have access to the information they need, when they need it, to support better outcomes for local people;
- good decision making is supported by an information sharing framework providing staff with clear direction; and
- unnecessary appointments and admissions can be avoided.

The principles of the framework were to:

a) identify the appropriate lawful basis for information sharing;
b) provide the basis for security of information and the legal requirements associated with information sharing;
c) address the need to develop and manage the use of Information Sharing Agreements (ISAs);
d) encourage flows of personal data and develop good practice across integrated teams;
e) provide the basis for county-wide processes which will monitor and review data flows; and information sharing between partner services;

f) protect partner organisations from unlawful use of personal data; and
g) reduce the need for individuals to repeat their story when receiving an integrated service.

KEY LEARNING FROM THE INTRODUCTION OF THE FRAMEWORK

- Staff need to be empowered to feel confident about sharing information between partners. Senior leaders need to be visible to give staff the confidence to share patient information.
- Internal culture needs to be supportive. The culture needs to be underpinned by strong values and ethos. It is essential that a learning culture is developed so that mistakes can be shared and learnt from rather than brushed aside. This learning includes developing formal training for all staff who were using an integrated care record, supported by the framework.
- Transparency needs to be established so that there is a collective understanding of how the data will be shared and by whom it will be shared. Staff need to have clarity around their roles and responsibilities and the benefits of sharing information.
- Need to develop a culture of appropriate sharing in plain English. Messages need to be simplified to avoid confusion and jargon needs to be reduced.

Lawful basis: legal obligation; fairness and transparency; individual rights

Data sharing required by law

A local authority is required by law to participate in a nationwide anti-fraud exercise that involves disclosing personal data about its employees to an anti–fraud body. The exercise is intended to detect local authority employees who are illegally claiming benefits that they are not entitled to.

Even though the sharing is required by law, the local authority should still inform any employees affected that data about them is going to be shared and should explain why this is taking place, unless this would prejudice proceedings.

The local authority should say what data items are going to be shared – names, addresses and National Insurance numbers - and provide the identity of the organisation they will be shared with.

There is no point in the local authority seeking employees' consent for the sharing because the law says the sharing can take place without consent. The local authority should also be clear with its employees that even if they object to the sharing, it will still take place.

The local authority should be prepared to investigate complaints from any employees who believe they have been treated unfairly because, for example, their records have been mixed up with those of an employee with the same name.

Lawful basis; special category data; fairness and transparency; accountability

Considerations in relation to a healthcare data sharing agreement

Relevant parts of the NHS and social services in a region share personal information with the region's police force to ensure that mental health service users who are in contact with the police are safeguarded and have access to appropriate specialist support.

The partner organisations have developed a data sharing agreement to support their joint mental health policy. Depending on the circumstances of each case, the lawful basis may be consent or a task carried out in the public

interest. The data sharing agreement clearly identifies the various pieces of legislation that each partner relies on to specify their public functions and the provisions they need to meet if relying on consent. As special category data is likely to be necessary for referrals, they have also identified Article 9 conditions. The data sharing agreement reminds all parties to maintain the rights and dignity of patients, their carers and families, involving them in risk assessments wherever possible whilst also ensuring their safety and that of others.

Data sharing agreement; accountability; information rights

Public sector bodies sharing data to provide a co-ordinated approach

Personal information is shared between two councils, their local schools and colleges, housing providers, relevant community organisations, the local job centres and careers service in order to identify young people who already have been, or are at high risk of, disengaging from education, employment or training. By sharing the information, the partner organisations can ensure a co-ordinated approach to providing the most appropriate support to the young person to encourage them back in to education, work or training.

The partners used a data sharing agreement to set out their purpose, lawful bases and the information to be shared. The agreement included a section on how to handle data subjects' rights, and agreed shared security standards; the partners also updated their privacy notices. To quality assure their agreement, they shared it with a regional group of data protection practitioners for feedback. A timescale was also set for the partners to regularly review the agreement to ensure it stayed up to date and fit for purpose.

Data sharing under the Digital Economy Act 2017 powers

Both Companies House (CH) and Her Majesty's Revenue and Customs (HMRC) collect annual accounts from businesses. The accounts contain key corporate and financial information related to the company, such as the names of company directors or financial reporting figures showing their profit and loss.

There is the opportunity, however, for the same company to file a different set of accounts to each of the two organisations. By filing inflated accounts at Companies House and lower figures at HMRC, they will simultaneously

increase their creditworthiness with financial institutions and wider government whilst also reducing tax liabilities.

Until 2018, restrictions on data sharing had prevented HMRC and Companies House from sharing company accounts for comparison. With the introduction of the Digital Economy Act 2017, however, a permissive legal gateway was provided to share information to combat fraud.

Prior to sharing information, Companies House and HMRC met to draw up the governance and processes:

- They would share information as a pilot.
- Both parties designed and agreed a data specification.
- They completed a data protection impact assessment to ensure they considered proportionality and fair processing.
- Both parties signed an information sharing agreement.

HMRC disclosed the first set of company accounts information to Companies House in October 2018 – the very first transfer of data under the Digital Economy Act powers.

The pilot sought to address the fraud problem through ten defined data analytics and compliance work streams, each one relating to a mode of behaviour indicating false account filing and fraudulent activity. For the first time the pilot utilised qualitative analysis to access and compare key words and phrases. Further to this, the pilot also utilised Companies House back office data to uncover previously hidden links between companies, combined for the first time with HMRC intelligence.

The data-sharing pilot identified £14.6m of savings, with a further £100.6m if the data share was embedded as business as usual. In addition, they identified over 3,500 sets of accounts as incorrect at Companies House, thereby improving the integrity of the data held on the register.