事业档案管理的隐私保护与个人信息管理研究

叶林芝

河北省承德市自然资源和规划局不动产登记中心

摘　要：事业档案管理是组织中一个重要的工作流程，涉及大量的个人信息的处理和管理。为了保护个人隐私权，事业档案管理需要遵循一系列的隐私保护原则和规范。此外，我们还将讨论事业档案管理中的隐私保护技术和政策措施，包括数据加密和安全存储、访问权限控制和身份验证技术以及制定隐私保护政策、员工培训和教育等。通过采取这些措施，事业档案管理可以更好地保护个人隐私，确保个人信息的安全和合法处理。

关键词：事业档案管理；隐私保护；个人信息管理

【DOI】10.12252/j.issn.2096-6288.2022.05.179

引言

随着信息技术的快速发展，事业档案管理在现代组织中扮演着重要角色。然而，个人隐私保护与个人信息管理问题也引起了广泛的关注。本文旨在探讨事业档案管理的隐私保护与个人信息管理，提出相关研究问题，并探讨可能的解决方案。

一、事业档案管理的概述

（一）事业档案管理的定义和重要性

事业档案管理对于组织来说具有重要的意义。首先，事业档案管理是人力资源管理的基础。通过对员工职业生涯的信息记录和管理，组织可以了解员工的背景、能力、经验和潜力，有针对性地进行培养和发展，为组织的长期发展提供人才支持。其次，事业档案管理是组织内部控制的重要手段之一。通过严格管理和保护档案信息，组织可以提高决策的科学性和透明度，减少内部管理风险。此外，事业档案管理还可以帮助员工进行个人职业规划和发展，提高员工的工作动力和满意度。

（二）事业档案管理中的个人信息收集和存储

事业档案管理中的个人信息收集和存储是整个档案管理过程的重要环节。在收集个人信息时，组织需要遵循以下原则：合法性、目的明确、选择性、最小化和及时性。也就是说，组织应该合法地收集个人信息，明确收集信息的目的，并且仅限于实现这些目的所必需的信息，不得过度收集和使用个人信息。为了保护个人信息的安全和隐私，事业档案管理通常采用以下措施进行信息存储与保护：

（1）物理安全措施

包括对纸质档案的存放、传递和销毁进行控制，如密封存储盒、专用密封柜、封条等。同时，还要确保档案室环境的安全，如门禁控制、视频监控等。

（2）电子安全措施

包括对电子档案的加密、备份和权限控制。组织可以采用加密算法保护敏感信息，定期备份数据以防止意外丢失，并通过权限控制确保只有授权人员才能访问敏感档案信息。

（3）审计和监控机制

事业档案管理应建立完善的审计和监控机制，对档案访问记录、修改历史等进行监测和审计，及时发现和防范未授权的访问和操作。

（4）员工培训和意识提升

组织应加强员工的信息安全培训和意识提升，使其了解个人信息的重要性和保护措施，并且严格遵守相关的信息保护规定和政策。

二、个人隐私保护问题

（一）个人隐私的含义和重要性

个人隐私是指个人对于自己的个人信息、身体、家庭、住所等方面的权利，包括保护个人信息不被滥用、泄漏或不合法收集使用。个人隐私的重要性在不断增强，尤其是在数字化时代。个人隐私的保护是一个基本人权，对于维护公民的尊严、自由和自主权具有关键地位。个人隐私保护是维护个人尊严和自主权的基础。每个人都有权决定自己的个人信息是否被公开，以及如何使用和处理这些信息。保护个人隐私可以避免身份盗窃、欺诈和其他不法行为对个人造成的威胁。有了隐私保护，个人可以更安心地使用各种服务和参与社交活动。个人隐私的保护是公民权利和自由的基石。它涉及个人在社会、政治、经济等方面的自由和权利，如言论自由、信仰自由、人身自由等。

（二）事业档案管理中可能存在的个人隐私泄漏问题

（1）非授权访问

如果事业档案管理系统没有足够的权限控制和访问限制措施，未经授权的人员有可能获取和使用个人档案信息，从而导致个人隐私泄漏。因此，建立有效的访问权限控制机制，确保只有经过授权的人员才能访问敏感

信息，是非常重要的。

（2）数据安全漏洞

事业档案管理系统中存在数据安全漏洞会给个人隐私带来风险。例如，弱密码、网络攻击等都可能导致数据被黑客或其他不法分子窃取。为了保护个人隐私，需要采取一系列的安全措施，如加密技术、防火墙等，确保个人档案信息的安全存储和传输。

（3）数据共享与合作

在事业档案管理的跨部门、跨组织合作中，数据共享协议的缺失或不明确可能导致数据共享滥用或不当使用的问题。在进行数据共享时，应制定明确的数据共享协议，明确数据使用的目的和范围，避免个人档案信息被滥用。

（4）数据匿名化问题

为了保护个人隐私，事业档案管理中的个人信息常常需要进行匿名化处理。然而，如果匿名化不彻底或技术手段不到位，有可能通过其他信息还原出个人身份，从而导致个人隐私泄漏。因此，在数据匿名化时，需要采用高效的技术手段，确保个人信息无法被还原

三、个人信息管理原则与规范

（一）个人信息管理的基本原则

个人信息管理的基本原则是确保合法、公正、透明、安全和自主。以下是一些常见的个人信息管理原则：

合法性原则：个人信息的收集、存储、处理和使用必须依法进行，要符合相关的法律法规和政策规定。

公正原则：个人信息的处理应当公平、诚实、和善意地进行，不得采用虚假或误导的手段获取个人信息。

透明原则：个人信息管理者应向个人提供清晰、明确的信息收集和使用说明，明确告知处理个人信息的目的、方式和范围。

安全原则：个人信息管理者应采取合理的安全措施，防止个人信息被未经授权的访问、泄漏、篡改或损坏。

自主原则：个人信息管理者应尊重个人隐私权，让个人能够自主决定自己的个人信息是否提供，以及如何使用和处理这些信息。

（二）相关法律法规和行业标准

为了保护个人信息的安全和隐私权，许多国家和地区都制定了相关的法律法规和行业标准。以下是一些重要的法律法规和行业标准：

（1）欧洲通用数据保护条例（GDPR）

该条例于2018年生效，适用于欧盟成员国及其他经济体。它规定了个人信息处理的基本原则和要求，并对个人选择、透明度、安全性和违规处罚等方面做出明确规定。

（2）加利福尼亚消费者隐私法（CCPA）

该法于2020年生效，适用于加利福尼亚州的企业。它赋予消费者更多关于其个人信息收集和使用的控制权，并要求企业提供透明的隐私政策和机制。

（3）国际标准化组织（ISO）发布的个人信息管理体系标准ISO27701

该标准为组织建立和实施个人信息管理体系提供了指导，帮助组织管理个人信息的合规性和安全性。

各个国家和地区还有自己的相关法律法规和行业标准，例如美国的HIPAA法案（适用于医疗信息）、中国的《个人信息安全规范》等。

个人信息管理者应当遵守所在地区的相关法律法规和行业标准，并采取合理的措施确保个人信息的安全、合法和公正处理。同时，他们还应该建立健全的个人信息保护制度，指定专门的个人信息保护责任人，并通过培训和教育提高员工的个人信息保护意识。

四、事业档案管理的隐私保护技术

（一）数据加密和安全存储

数据加密和安全存储是事业档案管理中常用的隐私保护技术之一。通过对个人档案中的敏感信息进行加密，可以确保个人档案信息在传输和存储过程中不被未经授权的访问者获取。数据加密是将数据转化为密文的过程，只有具备解密密钥的授权人员才能解读和使用这些数据。在数据加密中，对称加密和非对称加密都有所应用。对称加密使用同一个密钥来进行数据加密和解密，而非对称加密则使用一对密钥，公钥用于加密数据，私钥用于解密。无论是对称还是非对称加密，选择合适的加密算法和密钥管理方案非常重要，以确保加密的安全性和可靠性。此外，在数据存储方面，采用安全的存储设备和系统也是非常重要的。例如，使用防火墙、入侵检测系统和数据备份等措施可以提高数据的安全性和可靠性。防火墙可以监控和控制数据流量，阻止未经授权的访问，入侵检测系统可以及时发现和报警可能的数据安全事件，而数据备份则可以保证数据在意外损坏或灾难发生时的恢复能力。

（二）访问权限控制和身份验证技术

通过确定并限制只有经过授权的人员才能访问和操作个人档案信息，可以减少内部和外部的风险。访问权限控制涉及对人员分配不同的权限级别和角色，根据需求对其进行授权，并建立访问控制列表来限制访问范围。员工可以根据自己的角色和职责获得相应的访问权限。身份验证技术用于验证个人身份的真实性，以确保

只有经过身份验证的人员才能获得访问权限。常用的身份验证技术包括用户身份验证、双因素认证等。用户身份验证通常涉及使用用户名和密码进行验证，在此基础上可以使用其他验证因素，如指纹识别、虹膜识别、声纹识别等，以提高身份验证的可靠性。数据加密和安全存储以及访问权限控制和身份验证技术在事业档案管理中起着重要的隐私保护作用。通过这些技术的应用，事业档案管理组织可以确保个人档案信息的机密性和完整性，减少个人隐私信息被未授权访问和使用的风险。然而，为了充分发挥这些技术的效果，事业档案管理组织还应该建立合适的策略和流程，并保证技术的合理配置和管理，以确保隐私保护机制的有效实施。

五、事业档案管理的隐私保护政策与措施

（一）隐私保护政策的制定与实施

事业档案管理组织应制定明确的隐私保护政策，并确保其与相关法律法规相一致。该隐私保护政策应包括以下内容：

（1）收集和使用个人信息的目的

明确个人档案信息的收集目的，并且仅限于实现这些目的。例如，个人档案信息的收集可能是为了进行人力资源管理，提供合适的职位匹配，评估员工的表现等。

（2）使用和存储个人信息的范围和期限

明确个人档案信息的使用范围和存储期限，确保个人信息仅在合法、必要的范围内使用，并在不再需要时进行安全删除或匿名化处理。

（3）个人权利保护

明确个人对个人档案信息的访问、更正、删除等权利，以及个人如何行使这些权利的流程和方法。例如，组织应为员工提供合适的渠道，使他们可以自主地访问和修改自己的个人档案信息。

（4）个人信息保护责任分工

明确在组织内的个人信息管理责任分工，包括指定隐私保护负责人或团队，确保隐私保护工作得到有效执行。

（5）员工行为准则

建立员工行为准则，要求员工遵守相关的法律法规和隐私保护政策，保护个人档案信息的安全和机密性。

隐私保护政策应公开透明，并通过适当的渠道向相关方提供，如组织内部网站、员工手册等。此外，事业档案管理组织应定期审查和更新隐私保护政策，以及监测其实施情况，确保其与新的隐私保护要求和技术发展相适应。

（二）员工培训和教育

事业档案管理组织应定期进行员工培训和教育，提高员工对个人隐私保护的意识和重视程度。培训内容可以包括以下方面：

（1）隐私保护意义

介绍个人隐私的重要性和保护个人隐私的理由，以使员工充分认识到个人隐私保护的意义和价值。

（2）隐私政策要求

详细介绍组织制定的隐私保护政策和相应的要求，包括个人信息的收集和使用范围、访问权限和数据存储期限等。

（3）安全措施的操作指南

培训员工如何正确操作和使用安全措施，例如如何处理敏感信息、如何设置安全密码等，加强个人档案信息的安全保护。

（4）个人信息事件应急处理

培训员工在个人信息泄漏或违规使用等紧急事件发生时应如何快速应对和处理，以减少潜在的损失。

通过这些培训和教育，员工将更深入地了解隐私保护的重要性，并了解如何正确处理和保护个人档案信息。他们将具备遵守隐私政策和相关法律法规的能力，有效地履行其个人信息保护的职责。

结束语

在当前信息化的时代，个人隐私保护面临了越来越大的挑战，事业档案管理组织有责任采取措施来保护员工和个人的隐私权益。本文讨论了事业档案管理中存在的潜在个人隐私泄漏问题，并提出了加强数据加密和安全存储、访问权限控制和身份验证技术等措施。此外，制定和实施明确的隐私保护政策，以及进行员工培训和教育，也是保护个人隐私的重要手段。个人隐私保护不仅仅是一种法律法规的要求，更是对个人权利和尊严的尊重。通过合适的技术措施和行为准则，事业档案管理组织可以最大限度地降低个人隐私泄漏的风险。同时，组织也需要不断更新隐私保护政策和相关技术，以应对新的隐私保护挑战。

参考文献

[1]吕焱.加强事业单位档案管理质量建设的研究[J].黑龙江档案，2022（01）：192-194.

[2]邹洪伟.大数据时代档案用户信息隐私权保护的思考[J].黑龙江档案，2021（01）：192-193.

[3]王敏.对档案开放与档案隐私保护的思考[J].档案管理，2020（04）：56-57.

作者简介：叶林芝，女，1972年11月10日出生，河北省承德市双桥区人，河北省承德市自然资源和规划局不动产登记中心闫营子档案馆馆长，中央党校函授学院毕业，政法专业，大学本科学历。