Stellungnahme für die Installation einer elektronischen Zutrittskontrolle bei der Stadt Kitzingen

Bisherige Situation:

Bei der Ersterfassung zum Datenschutz vom 06.08. – 08.08.2019 bei der Stadt Kitzingen wurde vom Datenschutzbeauftragten festgestellt, dass die Zutrittskontrolle nur mangelhaft umgesetzt wurde:

- die Aus-, Weiter- und Rückgabe von Schlüsseln wurde nur lückenhaft dokumentiert
- zu viele Generalschlüssel sind im Umlauf
- das Trennungsgebot (Artikel 32 Abs. 1 litte b DSGVO) wurde teilweise missachtet
- verlorengegangene bzw. nicht wieder auffindbare Schlüssel wurden ersetzt, Schlösser wurden nicht ausgetauscht

Ein großer Schlüsselbestand lässt sich auf Dauer nicht effizient mit Karteikarten, Schlüsselbüchern oder Excel-Tabellen verwalten. Ab einer bestimmten Organisationsgröße und Mitarbeiterzahl macht ein in ordentlichen Bahnen laufendes, digitales Verfahren zur Ausgabe, Weitergabe, Rückgabe und Dokumentation von physischen oder elektronischen Schlüsseln, die per se Zutrittsrechte zu Räumen und Gebäuden repräsentieren, Sinn. Daher befürwortet der Datenschutzbeauftragte den Vorschlag der Stadt Kitzingen die Zutrittskontrolle in Zukunft über eine **zentrale, softwaretechnisch gesteuerte elektronische Schließanlage** zu lösen.

Gesetzliche Vorgaben:

Beim Thema Schlüsselverwaltung muss nicht nur die Aus- und Weitergabe von Schlüsseln geregelt und dokumentiert werden. Auch der Entzug von Zutrittsberechtigungen sowie weitere Besonderheiten sind zu beachten: Tresore unter Doppelverschluss, lückenlose Dokumentation schutzbedürftiger Räume und Vertretungsregelungen in Krankheits- oder Urlaubszeiten. Dabei greifen von gesetzlicher Seite vor allem folgende Vorschriften:

- *§ 64 BDSG*
  Anforderungen an die Sicherheit der Datenverarbeitung
  (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die **erforderlichen technischen und organisatorischen Maßnahmen** zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik [(1)] zu berücksichtigen.

  (2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen,

soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die **Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- *Artikel 24 DSGVO*
  Verantwortung des für die Verarbeitung Verantwortlichen
  (1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen um**, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

- *Artikel 32 DSGVO*
  Sicherheit der Verarbeitung
  (1) Unter Berücksichtigung des Stands der Technik, der Implementierungs-kosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

  a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

  b) die Fähigkeit, die **Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

(1) Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist dem Ministerium für Inneres angegliedert, existiert seit über 25 Jahren und ist zentraler Sicherheitsdienstleister des Bundes. Es befasst sich mit der Identifikation neuer Lücken in der IT-Sicherheit des Bundes und veröffentlicht Standards zu deren Vermeidung. Im IT-Grundschutzkatalog des BSI, Maßnahmenkatalog M 2.6 (Vergabe von Zutrittsberechtigungen), ist hinterlegt, dass Zutrittsrechte zu geschützten Räumen nach dem Kenntnis-nur-bei-Bedarf-Prinzip zu vergeben sind. Darüber hinaus sind sowohl die Vergabe als auch die Rücknahme von Zutrittsrechten zu dokumentieren.

Stellungnahme:

Die Zutrittskontrolle ist eine elementare Einrichtung, die in keiner Kommune fehlen darf. Sie soll verhindern, dass unbefugte Personen den physikalischen Zutritt zu personenbezogenen Daten erhalten. Dies bedeutet auch, dass nur diejenigen Mitarbeiter Zutritt zu bestimmten, sensiblen Bereichen (z.B. Serverraum oder Personalabteilung) haben sollen, die dazu berechtigt sind.

Ein Zutrittskontrollsystem ist ein elektronisches Hilfsmittel, das für die Zutrittskontrolle verantwortlich ist und automatisch prüft, ob die Berechtigungen einer Person vorhanden sind, um ein bestimmtes Gebäude, einen Bereich oder Raum betreten zu dürfen. Gleichzeitig mit der Zutrittsberechtigung wird auch die Dauer dieser Berechtigung festgelegt. Diese kann also einmalig, zeitlich begrenzt oder unbegrenzt sein. Ein Zutrittskontrollsystem erhöht die Sicherheit erheblich und unterstützt die betrieblichen Abläufe.

Eine zentrale, softwaretechnisch gesteuerte elektronische Schließanlage hat hierbei folgende Vorteile

- besonders einfache Handhabung
- uneingeschränkte Skalierbarkeit
- Flexibilität im Einsatz
- bei Verlust kein Austausch des gesamten Systems erforderlich
- Erweiterbarkeit der Funktionalität

Zu beachten ist:

Bei der Installation elektronischer Zutrittskontrollsysteme ist darauf zu achten, dass nur ein Minimum an Daten verarbeitet wird, eindeutige Verwendungs-regelungen für die gespeicherten Daten getroffen werden und deren Einhaltung revisionsfähig geprüft wird.

Da aufgrund der aus dem Zutrittskontrollsystem gewonnenen Daten grundsätzlich eine Bewegungsprofil erstellt werden könnte, bedarf es der Einwilligung jedes einzelnen Mitarbeiters. Der Personalrat ist bei Einführung, Anwendung und erheblicher Änderung der elektronischen Schließanlage zu beteiligen. Ebenso bedarf der erstmalige Einsatz einer elektronischen Schließanlage der vorherigen schriftlichen datenschutzrechtlichen Freigabe durch den Datenschutz-beauftragten. Nicht zuletzt aus Transparenzgründen empfehle ich in diesem Zusammenhang stets, eine Dienstvereinbarung im Sinne des Art. 73 BayPVG.