

改正

令和6年3月11日規程第4号

八尾市保有個人情報保護管理規程

目次

- 第1章 総則（第1条・第2条）
- 第2章 管理体制（第3条—第9条）
- 第3章 教育研修（第10条）
- 第4章 職員の責務（第11条）
- 第5章 保有個人情報の取扱い（第12条—第20条）
- 第6章 保有個人情報を取り扱う情報システムにおける安全の確保等（第21条—第35条）
- 第7章 サーバ等設置室の安全管理（第36条・第37条）
- 第8章 保有個人情報の提供及び業務の委託等（第38条—第40条）
- 第9章 サイバーセキュリティの確保（第41条）
- 第10章 安全確保上の問題への対応（第42条・第43条）
- 第11章 監査及び点検の実施（第44条—第46条）

附則

第1章 総則

（趣旨）

第1条 この規程は、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第7条の規定に基づく個人情報の保護に関する基本方針、法第66条及び行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）第12条の規定に基づき、本市の保有する個人情報（以下「保有個人情報」という。）の適切な管理のために必要な措置について定めるものとする。

（定義）

第2条 この規程で使用する用語は、法及び番号法で使用する用語の例による。

- 2 前項に定めるもののほか、この規程において「情報システム」とは、八尾市情報セキュリティ規則（平成24年八尾市規則第21号）第2条第2号に規定する情報システムをいう。

第2章 管理体制

(総括個人情報保護管理者)

第3条 本市に、総括個人情報保護管理者（以下「総括保護管理者」という。）を置くこととし、副市長をもって充てる。

2 総括保護管理者は、本市の職員（派遣労働者を含む。以下同じ。）に対する保有個人情報の管理に関する事務の指導監督等を行うとともに、本市における保有個人情報等の管理に関する事務を総括する任に当たる。

3 総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡、調整等を行うため必要があると認めるときは、関係職員を構成員とする委員会を設け、定期又は随時に開催することができる。なお、必要に応じて情報セキュリティ等について専門的な知識及び経験を有する者等の参加を求めることができる。

(部個人情報保護管理者)

第4条 部等に、部個人情報保護管理者（以下「部保護管理者」という。）を置くこととし、各部署の長をもって充てる。

2 部保護管理者は、当該部等における保有個人情報の管理に関する事務の運営につき、監督を行う任に当たる。

(個人情報保護管理者)

第5条 課等に、個人情報保護管理者（以下「保護管理者」という。）を置くこととし、各課等の長をもって充てる。

2 保護管理者は、当該課等における保有個人情報の適切な管理を確保する任に当たる。なお、保有個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる。

(個人情報保護担当者)

第6条 課等に、個人情報保護担当者（以下「保護担当者」という。）を置くこととし、情報公開推進員をもって充てる。

2 保護担当者は、保護管理者を補佐し、当該課等における保有個人情報の管理に関する事務を担当する。

(特定個人情報事務取扱担当者)

第7条 特定個人情報を取り扱う課等に、特定個人情報を取り扱う職員として特定個人情報事務取扱担当者（以下「事務取扱担当者」という。）を置くこととし、事務取扱担当者及びその役割並びに当該事務取扱担当者が取り扱う特定個人情報の範囲は、保護管理者が指定する。ただし、部

保護管理者が必要と認めるときは、当該部等における事務取扱担当者を定めることができる。

(特定個人情報の取扱いに係る組織体制の整備)

第8条 部保護管理者又は保護管理者は、特定個人情報の取扱いに関し、次の各号に掲げる組織体制を整備する。

- (1) 特定個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任体制
 - (2) 特定個人情報の漏えい、滅失、毀損等（以下「漏えい等」という。）の事案の発生又は兆候を把握した場合、職員がこの規程に違反している事実又は兆候を把握した場合その他安全確保の上で問題となる事案が発生した場合の保護管理者への報告連絡体制
 - (3) 特定個人情報の漏えい等の事案の発生又は兆候を把握した場合の対応体制
- (個人情報保護監査責任者)

第9条 本市に個人情報保護監査責任者（以下「監査責任者」という。）を置くこととし、総務部長をもって充てる。

- 2 監査責任者は、本市における保有個人情報の管理の状況について監査する任に当たる。
- 3 総務部における保有個人情報の管理の状況について監査を行う場合は、総務部長がその職務を代理する者を指名するものとする。

第3章 教育研修

(教育研修の実施)

第10条 総括保護管理者は、保有個人情報を取り扱う職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

- 2 総括保護管理者は、保有個人情報に係る情報システムを取り扱う職員に対し、保有個人情報の適切な管理のために、当該情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。
- 3 総括保護管理者は、前2項に規定する教育研修を部保護管理者に行わせることができる。
- 4 保護管理者は、当該課等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者又は部保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

第4章 職員の責務

(法令等の遵守)

第11条 職員は、法、番号法その他の関係法令並びに総括保護管理者、部保護管理者及び保護管理者の指示に従い、保有個人情報を取り扱わなければならない。

第5章 保有個人情報の取扱い

(アクセス制限)

第12条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限（以下「アクセス権限」という。）を有する職員の範囲及び権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限らなければならない。

2 アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。

3 職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で、保有個人情報にアクセスしてはならず、業務上の目的であってもアクセスは必要最小限としなければならない。

(複製等の制限)

第13条 保護管理者は、業務上の目的で職員が次の各号に掲げる行為を行おうとする場合は、当該保有個人情報の秘匿性等その内容に応じて、当該行為を必要最小限に限らなければならない。

(1) 保有個人情報の複製

(2) 保有個人情報の送信

(3) 保有個人情報が記録されている媒体の外部への送付又は持ち出し

(4) 前3号に掲げるもののほか保有個人情報の適切な管理に支障を及ぼすおそれのある行為

(誤りの訂正等)

第14条 職員は、保有個人情報の内容に誤りを発見した場合には、保護管理者の指示に従い、訂正等を行う。

(媒体の管理等)

第15条 職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行う。

2 職員は、保有個人情報が記録されている媒体を外部へ送付し、又は持ち出す場合には、原則として、パスワード、ＩＣカード、生体情報等（以下「パスワード等」という。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。

(誤送付等の防止)

第16条 職員は、保有個人情報を含む電磁的記録若しくは媒体の誤送信、誤送付若しくは誤交付又はウェブサイト等への誤記載を防止するため、個別の事務及び事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認、チェックリストの活用等の必要な措置を講ずる。

(廃棄等)

第17条 職員は、保有個人情報記録されている媒体が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該保有個人情報の消去又は当該媒体の廃棄を行う。

2 保有個人情報の消去又は保有個人情報記録されている媒体の廃棄を委託する場合（2以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取る等、委託先において消去及び廃棄が確実に行われていることを確認する。

（保有個人情報の取扱状況の記録）

第18条 保護管理者は、保有個人情報の秘匿性等その内容に応じた台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する。

（外的環境の把握）

第19条 保有個人情報が外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講ずる。

（取扱区域）

第20条 部保護管理者又は保護管理者は、特定個人情報を取り扱う事務を実施する区域を明確にし、物理的な安全管理措置を講ずる。

第6章 保有個人情報を取り扱う情報システムにおける安全の確保等

（アクセス制御）

第21条 保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下この章において同じ。）の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずる。

2 保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。

（アクセス記録）

第22条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、定期的に分析するために必要な措置を講ずる。

2 保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

（アクセス状況の監視）

第23条 保護管理者は、保有個人情報の秘匿性等その内容及び量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告の表示がなされる機能の設定、当該設定の定期的な確認等の必要な措置を講ずるよう努めるものとする。

(管理者権限の設定)

第24条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を必要最小限とする等の必要な措置を講ずる。

(外部からの不正アクセスの防止)

第25条 保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。

(不正プログラムによる漏えい等の防止)

第26条 保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置を講ずる。

(情報システムにおける保有個人情報の処理)

第27条 職員は、保有個人情報について、一時的な加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去しなければならない。

2 保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

(暗号化等)

第28条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の暗号化等を行うために必要な措置を講ずる。

2 職員は、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化又はパスワードの付与を行うよう努めるものとする。

(記録機能を有する機器及び媒体の接続制限)

第29条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器及び媒体の情報システム端末等への接続の制限等の必要な措置を講ずる。

(端末の限定)

第30条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う情報システム端末を限定するために必要な措置を講ずる。

(端末の盗難防止等)

第31条 保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。

2 職員は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではない。

(第三者の閲覧防止)

第32条 職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないように、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

(入力情報の照合等)

第33条 職員は、保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。

(バックアップ)

第34条 保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散して保管するために必要な措置を講ずる。

(情報システム設計書等の管理)

第35条 保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないように、その保管、複製、廃棄等について必要な措置を講ずる。

第7章 サーバ等設置室の安全管理

(入退管理)

第36条 保護管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「サーバ等設置室」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。

2 保護管理者は、必要があると認めるときは、サーバ等設置室の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずる。

- 3 保護管理者は、サーバ等設置室及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能の設定、パスワード等の管理に関する定めの整備、パスワード等の読取防止等を行うために必要な措置を講ずる。

(サーバ等設置室の管理)

第37条 保護管理者は、外部からの不正な侵入に備え、サーバ等設置室に施錠装置等の措置を講ずる。

- 2 保護管理者は、災害等に備え、サーバ等設置室に、耐震等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保等の措置を講ずる。

第8章 保有個人情報の提供及び業務の委託等

(保有個人情報の提供)

第38条 保護管理者は、法第69条第2項第3号及び第4号の規定に基づき他の行政機関等以外の者に保有個人情報（特定個人情報を除く。次項及び第3項において同じ。）を提供する場合には、法第70条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わす。

- 2 保護管理者は、法第69条第2項第3号及び第4号の規定に基づき他の行政機関等以外の者に保有個人情報を提供する場合には、法第70条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。

- 3 保護管理者は、法第69条第2項第3号の規定に基づき他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、法第70条の規定に基づき、前2項に規定する措置を講ずる。

- 4 保護管理者は、番号法で限定的に明記されたときを除き、特定個人情報を提供してはならない。

(業務の委託等)

第39条 個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずる。また、契約書に次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。

- (1) 個人情報に関する秘密保持、目的外利用の禁止等の義務
- (2) 再委託の制限又は事前承認等再委託に係る条件に関する事項

- (3) 個人情報の複製等の制限に関する事項
 - (4) 個人情報の安全管理措置に関する事項
 - (5) 個人情報の漏えい等の発生時における対応に関する事項
 - (6) 委託終了時における個人情報の消去及び媒体の返却又は廃棄に関する事項
 - (7) 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
 - (8) 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）
- 2 保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。
- 3 保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容及び量に応じて、作業の管理体制及び実施体制並びに個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認する。
- 4 委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第1項の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施する。この場合において、保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。
- 5 保護管理者は、個人番号関係事務の委託先が再委託をする際には、委託する業務において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。
- 6 保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等の個人情報の取扱いに関する事項を明記する。

（匿名化措置）

第40条 保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生リスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容等を考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。

第9章 サイバーセキュリティの確保

（サイバーセキュリティの水準の確保）

第41条 保有個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保する。

第10章 安全確保上の問題への対応

(事案の報告及び再発防止措置)

第42条 保有個人情報の漏えい等安全確保の上で問題となる事案又は問題となる事案の発生のおそれを認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する。

2 保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセス及び不正プログラムの感染が疑われる端末等のLANケーブルを抜く等被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

3 保護管理者は、事案の発生した経緯、被害状況等を調査し、部保護管理者、総務部総務課長（以下「総務課長」という。）及び総務部総務課情報公開室長（以下「情報公開室長」という。）に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに部保護管理者、総務課長及び情報公開室長に当該事案の内容等について報告する。

4 部保護管理者は、前項の規定に基づく報告を受けた場合には、当該事案の内容、経緯、被害状況等を総括保護管理者に報告する。

5 総括保護管理者は、前項の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を市長に速やかに報告する。

6 情報公開室長は、第3項の規定に基づく報告が法第68条第1項に規定する場合には、当該事案の内容等について個人情報保護委員会に直ちに報告する。

7 保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずるとともに、同種の業務を実施している課等に再発防止措置を共有する。

(公表等)

第43条 市長は、保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合には、事案の内容、影響等に応じて、事実及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。

第11章 監査及び点検の実施

(監査)

第44条 監査責任者は、保有個人情報の適切な管理を検証するため、第2章から第10章までに定める措置の状況を含む保有個人情報の管理の状況について、定期的に又は必要に応じて監査を行い、その結果を総括保護管理者に報告する。

2 監査責任者は、前項の監査を総務課長に行わせることができる。

(点検)

第45条 保護管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経過、保管方法等について、定期的に又は必要に応じて点検を行い、必要があると認めるときは、その結果を部保護管理者に報告する。

2 前項の報告を受けた部保護管理者は、必要があると認めるときは、その結果を総括保護管理者に報告する。

(評価及び見直し)

第46条 総括保護管理者、部保護管理者及び保護管理者は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。

附 則

この規程は、令和5年4月1日から施行する。

附 則 (令和6年3月11日規程第4号)

この規程は、公布の日から施行する。