

狭山市における特定個人情報等の取扱いに関する管理規程

目次

- 第1章 総則（第1条・第2条）
- 第2章 管理体制（第3条一第7条）
- 第3章 職員の責務（第8条一第11条）
- 第4章 保有特定個人情報等の取扱い（第12条一第22条）
- 第5章 情報システムにおける安全の確保等（第23条一第36条）
- 第6章 情報システム室等の安全管理（第37条・第38条）
- 第7章 保有特定個人情報等に係る業務の委託等（第39条）
- 第8章 安全確保上の問題への対応（第40条・第41条）
- 第9章 監査及び点検の実施（第42条一第44条）
- 第10章 その他（第45条）

第1章 総則

（目的）

第1条 この規程は、市が保有する特定個人情報について、その適切な管理に関して必要な事項を定めることを目的とする。

（用語）

第2条 この規程において使用する用語は、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2条及び狭山市個人情報保護条例（平成15年条例第25号。以下「保護条例」という。）第2条の定めるところによる。

第2章 管理体制

（総括保護管理者）

第3条 総括保護管理者を置き、総務部長をもって充てる。

2 総括保護管理者は、市が保有する個人番号及び特定個人情報（以下「特定個人情報等」という。）の管理に関する事務を総括する。

（保護管理者）

第4条 保有特定個人情報等を取り扱う各所管に、保護管理者を置き、狭山市行政組織規則（平成7年規則第18号）第7条第1項に規定する課長及び同規則第3章に規定する出先機関等の長（課長職にある者に限る。）、狭山市教育委員会事務局組織規則（平成10年教育委員会規則第5号）第5条第1項に規定する課の長及び同規則第2条第2項に規定する機関又は施設の長（課長職にあるものに限る。）、狭山市水道事業及び下水道事業管理規程（昭和58年公営企業管理規程第2号）第3条第1項に規定する課長、議会事務局次長、選挙管理委員会事務局長、監査委員事務局次長並びに農業委員会事務局長をもって充てる。

2 保護管理者は、各所管における保有特定個人情報等を適切に管理する。

3 保護管理者は、特定個人情報等を取り扱う職員（嘱託員及び臨時職員を含む。以下「職員」という。）及びその役割を指定する。

4 保護管理者は、職員が取り扱う特定個人情報等の範囲を指定する。

(保護担当者)

第5条 保有特定個人情報等を取り扱う各所管に、当該所管の保護管理者が指定する保護担当者を置く。

2 保護担当者は、保護管理者を補佐し、各所管における保有特定個人情報等の管理に関する事務を担当する。

(監査責任者)

第6条 監査責任者を置き、総務部次長をもって充てる。

2 監査責任者は、保有特定個人情報等の管理状況についての監査(外部監査を含む。)を行う。

(保有特定個人情報等の適切な管理のための体制)

第7条 保護管理者は、次に掲げる組織体制を整備する。

- (1) 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の総括保護管理者への報告連絡体制
- (2) 特定個人情報等の漏えい、滅失又はき損等(以下「情報漏えい等」という。)の事案の発生又は兆候を把握した場合の職員から総括保護管理者への報告連絡体制
- (3) 同一特定個人情報等を複数の所管で取り扱う場合の職務分担及び責任の明確化
- (4) 情報漏えい等の事案の発生又は兆候を把握した場合の体制

第3章 職員の責務

(教育研修)

第8条 総括保護管理者は、職員に対し、保有特定個人情報等の取扱いについて理解を深め、特定個人情報等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 個別情報システムを所管する保護管理者は、当該所管の職員に対し、保有特定個人情報等の適切な管理のために、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 保護管理者は、当該所管の職員に対し、保有特定個人情報等の適切な管理のために、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9条 職員は、番号法及び保護条例の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者及び保護管理者の指示に従い、保有特定個人情報等を取り扱わなければならない。

2 職員は、情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が当該規程等に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

3 総括保護管理者及び保護管理者は、特定個人情報等がこの規程に基づき適正に取扱われるよう職員に対して必要かつ適切な監督を行う。

4 職員は、この規程について不明な点を生じ、又は遵守し難い特別の事由が生じたときは、その旨を速やかに保護管理者に申し出て、必要な指示を受けなければならない。

第4章 保有特定個人情報等の取扱い

(アクセス制限)

第10条 保護管理者は、保有特定個人情報等にアクセスする権限を有する者を必要最小限の職員にしなければならない。

2 アクセス権限を有しない職員は、保有特定個人情報等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特定個人情報等にアクセスしてはならない。

(複製等の制限)

第11条 職員は、業務上の目的で保有特定個人情報等を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行う。

(1) 保有特定個人情報等の複製

(2) 保有特定個人情報等の送信

(3) 保有特定個人情報等が記録されている媒体の外部への送付又は持出し

(4) その他保有特定個人情報等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12条 職員は、保有特定個人情報等の内容に誤り等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。

(特定個人情報等の管理等)

第13条 職員は、保護管理者の指示に従い、保有特定個人情報等が記録されている電子媒体等を定められた場所の施錠ができるキャビネット等に保管する。

(特定個人情報等の廃棄等)

第14条 職員は、保有特定個人情報等又は保有特定個人情報等が記録されている電子媒体等(端末及びサーバに内蔵されているものを含む。)が不要となった場合には、保護管理者の指示に従い、当該保有特定個人情報等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体等の廃棄を行う。

2 保護管理者は、個人番号若しくは特定個人情報ファイルを消去し、又は電子媒体等を廃棄した場合には、消去し、又は廃棄した記録を保存する。また、これらの作業を委託(再委託含む。)する場合には、委託先が確実に消去し、又は廃棄したことについて、証明書等により確認する。

(保有特定個人情報等の取扱状況の記録)

第15条 保護管理者は、特定個人情報ファイルの取扱状況を確認する手段を整備し、当該特定個人情報等の利用及び保管等の取扱状況について記録するよう努める。

(個人番号の利用の制限)

第16条 保護管理者は、個人番号の利用に当たり、番号法等に定めた事務に限定する。

(個人番号の提供の求めの制限)

第17条 職員は、個人番号利用事務又は個人番号関係事務(以下「個人番号利用事務等」という。)を処理するために必要な場合その他番号法で定める場合を除き、個人番号の提供を求めてはならない。

(特定個人情報ファイルの作成の制限)

第18条 職員は、個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

(特定個人情報等の収集・保管の制限)

第 19 条 職員は、番号法第 19 条各号のいずれかに該当する場合を除き、特定個人情報等を収集し、又は保管してはならない。

(取扱区域)

第 20 条 保護管理者は、特定個人情報等を取扱う事務を実施する区域（以下（取扱という。）を明確にし、物理的な安全管理措置を講ずる。

第 5 章 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 個別情報システムを所管する保護管理者は、保有特定個人情報等(情報システムで取り扱うものに限る。以下第 6 章において同じ。)に、パスワード等(パスワード、ICカード、生体情報等をいう。以下同じ。)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。

2 前項の保護管理者は、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の整備(定期又は随時の見直しを含む。)、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、特定個人情報等へのアクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずる。また、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。

(外部からの不正アクセスの防止)

第 23 条 個別情報システムを所管する保護管理者は、保有特定個人情報等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、経路制御等の必要な措置を講ずる。

(情報漏えい等の防止)

第 24 条 保護管理者は、特定個人情報等を外部に送信する場合には、通信経路における情報漏えい等を防止するための措置を講ずる。

(不正プログラムによる漏えい等の防止)

第 25 条 個別情報システムを所管する保護管理者は、不正プログラムによる保有特定個人情報等の漏えい、滅失又はき損の防止のため、不正プログラムの感染防止等の必要な措置を講ずる。

(保有特定個人情報の処理)

第 26 条 職員は、保有特定個人情報について一時的に加工等の処理を行うため複製等を行う場合には、その対象者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する。

2 保護管理者は、前項の保有特定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 27 条 保護管理者は、保有特定個人情報等の暗号化等のために必要な措置を講ずる。

(入力情報の照合等)

第 28 条 職員は、入力原票と入力内容との照合、処理前後の当該保有特定個人情報

の内容の確認、既存の保有特定個人情報との照合等を行う。

(バックアップ)

第 29 条 個別情報システムを所管する保護管理者は、バックアップを作成し、分散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 30 条 個別情報システムを所管する保護管理者は、保有特定個人情報等に係る情報システムの設計書、構成図等の文言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。

(端末の限定)

第 31 条 個別情報システムを所管する保護管理者は、特定個人情報等の処理を行う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 32 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らない。

(第三者の閲覧防止)

第 33 条 職員は、端末の使用に当たっては、保有特定個人情報等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。

(記録機能を有する機器・媒体の接続制限)

第 34 条 個別情報システムを所管する保護管理者は、保有特定個人情報等の情報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・媒体の情報システム端末等への接続の制限(当該機器の更新への対応を含む。)等の必要な措置を講ずる。

(記録機能を有する媒体・書類の移送手段)

第 35 条 職員は、この規程の手續に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち出す必要が生じた場合には、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等安全な方策を講ずる。

第 6 章 情報システム室等の安全管理

(入退管理)

第 36 条 個別情報システムを所管する保護管理者は、保有特定個人情報等を取り扱う基幹的なサーバ等の機器を設置する部屋その他の区域(以下「情報システム室等」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、入退室の記録、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、監視設備による監視又は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若しくは検査等の措置を講ずる。また、保有特定個人情報等を記録する電子媒体等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 前項の保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。

3 第 1 項の保護管理者は、情報システム室等及び保管施設の入退室の管理について、

必要があると認めるときは、立入りに係る認証機能を設定し、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。

(情報システム室等の管理)

第 37 条 個別情報システムを所管する保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

2 前項の保護管理者は、災害等に備え、電算室等に、耐震、防火、防煙、防水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、配線の損傷防止等の措置を講ずる。

第 7 章 保有特定個人情報等に係る業務の委託等

第 38 条 保護管理者は、保有特定個人情報等の取扱いに係る業務を外部に委託する場合には、特定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必要な措置を講ずる。また、契約書等に、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及び実施体制並びに、特定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) 秘密保持義務
 - (2) 事業所内からの特定個人情報の持ち出しの禁止
 - (3) 特定個人情報の目的外利用の禁止
 - (4) 再委託における条件
 - (5) 情報漏えい等の事案が発生した場合の委託先等の責任
 - (6) 委託契約終了後の特定個人情報の返却又は廃棄
 - (7) 特定個人情報を取り扱う従業者の明確化
 - (8) 従業者に対する監督・教育
 - (9) 契約内容の遵守状況についての報告
 - (10) 市が必要と認める場合の委託先に対する実地調査
- 2 保護管理者は、個人番号利用事務等の全部又は一部を委託する場合には、委託先において、番号法に基づき市が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認する。
- 3 保護管理者は、個人番号利用事務等の全部又は一部の委託をする際には、「委託を受けた者」において、市が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行う。
- 4 保護管理者は、個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託をする際には、委託をする個人番号利用事務等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。
- 5 保有特定個人情報等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個人情報の取扱いに関する事項を明記する。

第 8 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 39 条 情報漏えい等の事案の発生又は兆候を把握した場合及び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等、安全確保上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有特定個人情報等を管理す

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講ずる。
- 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、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。
- 4 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、被害状況等を狭山市セキュリティポリシー第2章第4項第1号アに規定する最高情報セキュリティ責任者(CISO)（以下「最高情報セキュリティ責任者」という。）に速やかに報告する。
- 5 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。

(公表等)

第40条 最高情報セキュリティ責任者は、事案の内容、影響等に応じて、事実関係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9章 監査及び点検の実施

(監査)

- 第41条 監査責任者は、保有特定個人情報等の管理の状況について、定期に又は随時に監査(外部監査を含む。)を行い、その結果を総括保護管理者に報告する。
- 2 総括保護管理者は、監査の結果について必要があると認めるときは、最高情報セキュリティ責任者に報告する。

(点検)

- 第42条 保護管理者は、自ら管理責任を有する保有特定個人情報等の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行い、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。
- 2 総括保護管理者は、点検の結果について必要があると認めるときは、最高情報セキュリティ責任者に報告する。

(評価及び見直し)

第43条 保有特定個人情報等の適切な管理のための措置については、総括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。

第10章 その他

(委任)

第44条 この規程に定めるもののほか、この規程の実施のための手続その他について必要な事項は、別に定める。