

令和4年11月30日

世田谷区情報公開・個人情報保護審議会
会長 山田健太 様

世田谷区情報公開・個人情報保護審議会
小委員会委員長 斉木秀憲

個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱い
に関する運用上の細則等について（報告）

当委員会では、世田谷区情報公開・個人情報保護審議会へ諮問されている「個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱いに関する運用上の細則等」について、世田谷区情報公開・個人情報保護審議会条例第8条の規定に基づき設置された当委員会の委員により、その内容について検討しました。

その結果、別添「個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱いに関する運用上の細則等について 報告書」のとおりまとめましたので、報告いたします。

個人情報保護に関する法律の改正に伴う世田谷区の
個人情報の取扱いに関する運用上の細則等について

報 告 書

令和4年11月30日

世田谷区情報公開・個人情報保護審議会 小委員会

目次

1	条例要配慮個人情報の制定	1
2	個人情報保護管理基準	3
3	外部委託等の審査基準	4
4	開示請求手続の本人確認書類	5
5	死者の情報に関する開示請求基準	6
参考1	世田谷区情報公開・個人情報保護審議会小委員会 委員名簿	8
参考2	世田谷区情報公開・個人情報保護審議会小委員会 審議経過	9

1 条例要配慮個人情報の制定

(1) 現行の世田谷区個人情報保護条例(以下「条例」という。)と改正個人情報の保護に関する法律(以下「改正法」という。)の主な相違点

現行条例では、条例要配慮個人情報の定義規定はないものの、第7条で「収集禁止事項」を定め、原則として、思想、信条及び宗教に関する事項、社会的差別の原因となる事実に関する事項及び犯罪に関する事項の収集を禁止しており、例外的に審議会の意見を聴いて必要があると認められる場合等にこれらの情報を収集することを可能としている。一方、改正法では、第2条第3項で「要配慮個人情報」(人種、信条、社会的身分等)を定めている。また、第60条第5項で「地域の特性その他の事情に応じて、本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして地方公共団体が条例で定める記述等が含まれる個人情報」(いわゆる「条例要配慮個人情報」)を定め、「要配慮個人情報」に該当しない「条例要配慮個人情報」を条例で定めることができる旨規定している。

(2) これまでの間の議論の経緯

条例要配慮個人情報については、令和4年3月から同年5月までの間にかけて情報公開・個人情報保護審議会小委員会(以下「小委員会」という。)において審議し、さらに同年6月には情報公開・個人情報保護審議会(以下「審議会」という。)においても議論したものである。その際、区は、全所属への条例要配慮個人情報の該当性調査を行った結果、調査時点では区に条例要配慮個人情報に該当する情報は存在しないと報告した。

様々な議論を経た結果、改正法でカバーできる可能性が高い点、実務上具体的な事例が出てきた際に、再度検討して条例を改正することができる点及び条例要配慮個人情報の制定に伴う事務の取扱いが困難となる点、以上の三点の理由により条例要配慮個人情報の制定については見送るべきであるとの結論に至ったところであった。

今般の令和4年10月に設置された小委員会において、区から報告があり、区議会や区民意見提出手続(パブリックコメント)において、LGBTや国籍といった個人情報を条例要配慮個人情報として制定すべきとの意見が複数寄せられたとのことであった。区は、このことを重く受け止め、国の個人情報保護委員会に対して、区の立法措置として、「世田谷区多様性を認め合い男女共同参画と多文化共生を推進する条例」(以下「多様性条例」という。)があることを根拠に、LGBTや国籍といった

個人情報条例を要配慮個人情報に制定できるか否か照会したところ、同委員会から、一定程度の情報を要配慮個人情報に制定することも妨げられない旨の回答があったとのことである。

以上のことを踏まえ、区は総合的に勘案した結果、改正法第60条第5項に基づき、国籍、性的マイノリティに関する情報及びドメスティック・バイオレンスに関する情報を要配慮個人情報として制定することが適当であると考えに至ったため、再度、審議会に対して意見聴取を行うとしたものである。

(3) 主な意見

先の小委員会及び審議会では、条例を要配慮個人情報の制定の是非について、改正法でカバーできる可能性が高い点、実務上具体的な事例が出てきた際に、再度検討して条例を改正することができる点及び条例を要配慮個人情報の制定に伴う事務の取扱いが困難となる点、の三点を理由として見送ることが相当であるとしたものである。特に、区は三点目の理由を受け止め、より慎重に取り扱う必要がある。

国籍及び性的マイノリティに関する情報については、条例を要配慮個人情報として規定することも概ね問題ないと思われるものの、ドメスティック・バイオレンスに関する情報を要配慮個人情報として規定する場合は、非常に抽象的な内容であるがゆえ、特に慎重に議論すべきである。推知される情報は、一般的に条例を要配慮個人情報に該当しないと考えられる。よって、規定する場合には、抽象的な定義ではなく、具体的で、かつ、明瞭な定義が必要不可欠である。概念の明確性が重要である。

立法措置として区に多様性条例があることを前提として条例を要配慮個人情報に制定するという方向で進めるのであれば、条例を要配慮個人情報につき多様性条例の規定を引用することが望ましい。

多様性条例を根拠に進めることに異議はないものの、区の各部署における運用面で混乱が起らないようにして欲しい。

多様性条例のほかに、世田谷区パートナーシップの宣誓の取扱いに関する要綱がある。制定主体について、前者は区議会であり、後者は行政機関という乖離があることから、手続面で容易に対応が可能な後者に紐づけて条例を要配慮個人情報に制定することはバランスが良くない。条例を要配慮個人情報に制定する場合には、このような法形式の相違点も考慮すべきである。

(4) 考え方

多様性条例を根拠に、国籍、性的マイノリティ（多様性条例第2条

第6号に定める記述)及びドメスティック・バイオレンス(多様性条例第2条第7号に定める記述のうち、法第2条第3項に該当しないもの)の三点の個人情報を条例要配慮個人情報として制定することは相当である。

ただし、区内部における条例要配慮個人情報に関する事務運用等で混乱をきたすことは決してあってはならないため、令和5年4月以降、上記三点の情報を条例要配慮個人情報として適切に取り扱うことができるよう関係所管課と詳細を検討し、適切に職員周知を図ることを求める。

2 個人情報保護管理基準

(1) 趣旨

改正法第66条第1項により、各自治体は、「...保有個人情報の漏えい、滅失又は毀損の防止...個人情報の安全管理のために必要かつ適切な措置を講」ずべき義務が生じた。この規定を受け、国から「個人情報の保護に関する法律についての事務対応ガイド(行政機関等向け)」が周知され、各自治体は、当該ガイドに則り、安全管理措置を講ずべく個人情報保護管理基準を策定することとなったものである。

(2) 主な意見

第11(安全管理上の問題への対応)の「3 公表等」について、一度公表されてしまうと関係者の権利利益を害することが起こり得るため、事前手続の整備をする必要性があるかもしれない。

監査及び点検が実施されるとのことだが、これらの措置に対して審議会がどのように関与していくのか知りたい。

「個人情報を取り扱う業務の特記事項」及び「電算処理の業務委託契約の特記事項(兼電算処理の個人情報を取り扱う業務委託契約の特記事項)」において、いずれも損害賠償に係る規定が存在する。前者の対象に法令違反の場合も含めている一方で、後者の対象に法令違反の場合を含めていない理由が知りたい。

構成が複雑であるため、改正法や改正条例、当該管理基準等の位置関係が明瞭に理解できる図のようなものがあると尚良い。

(3) 考え方

前述のとおり、区が改正法第66条第1項及び「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」に基づき策定した個人情報保護管理基準の内容について異議はない。

ただし、「個人情報を取り扱う業務の特記事項」及び「電算処理の業務委託契約の特記事項（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）」の内容の整合を図るとともに、今後の周知を見据えて、改正法や改正条例、当該管理基準等の位置関係が明瞭にわかるよう工夫を凝らすことを要望する。

3 外部委託等の審査基準

(1) 趣旨

現行条例では、区の各所管課は、個人情報を取り扱う業務において外部委託、外部提供、目的外利用等を行う際に、原則として各個別案件ごとに事前に審議会へ諮問して承認され次第、開始している。

一方で、改正法では、外部委託については、第66条第1項により安全管理措置に関する基準を示し、委託先がこれを遵守することにより個人情報の適切な管理が担保されるとともに、区は外部提供及び目的外利用につき改正法第69条の規定を厳格に遵守することとなることから、各個別案件の審議会への事前諮問は許容されないところである。

このことを踏まえ、区が前述の個人情報保護管理基準を策定したうえで、各所管課が個人情報を取り扱う業務において外部委託、目的外利用及び外部提供を行う場合に、事前に審査することを可能とする各審査基準を策定するものである。

(2) 主な意見

各所管課は、審査基準で審査したうえで事業を実施した後、区政情報課に情報提供を行うような流れになるのか。

個人情報保護管理者である各課長が審査したうえで問題なければ、事業を実施できることとなるが、適正性が担保し得るのか。別票等の詳細なチェックリストでの審査をお願いしたい。

電子計算機への記録や回線結合といった、外部委託、外部提供及び目的外利用以外の現在の審議会への諮問事項の審査基準の策定の予定について知りたい。

審査基準の骨子は、どのようなものであるのか。

条例素案中、事務局である区政情報課から「事後報告を受け」、必要と認めた場合、「所管課に説明を求める」機能を有する「審議会」は、どのようなタイミングで「報告」を受けることとなるのか。また、必要と認めた場合、所管課に説明を求めるにあたって、当該案件に係る情報提供はどのようになされるのか。

「総括個人情報保護管理者」が設けるとされている「個人情報保護管理委員会」と「審議会」との機能・役割の分任の仕組みについて知りたい。

(3) 考え方

改正法の枠組みの中、外部委託、外部提供及び目的外利用につき、各所管課が個人情報を取り扱う際に審査する審査基準の方向性について異議はない。

ただし、各審査基準の別票を作成し、各所管課で詳細に審査できるようにすべきである。また、電子計算機への記録、回線結合といった外部委託、外部提供及び目的外利用以外の現在の審議会への諮問事項について、各所管課が事業実施前に混乱なく確認できるよう工夫を凝らす必要がある。

4 開示請求手続の本人確認書類

(1) 趣旨

現行条例施行規則において、開示請求手続の本人確認書類について詳細に定めているものの、改正法が施行される令和5年4月以降は、改正法に基づく開示請求を行うこととなることから、改正法及び政令の規定に沿った対応が求められる。については、改正法及び改正条例が施行される令和5年4月以降の開示請求手続の本人確認書類については、国が示した「個人情報の保護に関する法律についての事務対応ガイド」を参考とし、各自治体で具体的な本人確認書類を確定させる必要がある。

(2) 主な意見

特段意見なし。

(3) 考え方

まず、改正法では、開示請求時に確認する本人確認書類について、原則として、開示請求書に記載されている開示請求をする者の氏名及び住所

又は居所と同一の氏名及び住所又は居所が記載されていることを求めているため、この方針を採用することが相当である。

次に、なりすましが特に懸念される任意代理人による開示請求については、現行条例施行規則第10条（開示請求者の確認）において、保有特定個人情報における任意代理人による開示請求の場合に委任者本人の実印を押印した委任状及び当該実印に係る印鑑登録証明書を要求していることから、これを継続し、引き続き厳格な対応を行う方針を採用することが相当である。

最後に、本人による開示請求、法定代理人による開示請求及び任意代理人による開示請求の三点の開示請求について、区が提示した各請求時の具体的な本人確認書類は、改正法及び政令並びに現行条例の内容を鑑みた適正な内容であると認められるため、異議はない。

5 死者の情報に関する開示請求基準

（1）趣旨

現行条例も改正法も「個人情報」は、生存する個人に関する情報であり、死者に関する情報は含まれない。また、改正法では、改正条例に個人情報の定義として死者に関する情報を含める規定を設けることを許容していない。ただし、死者に関する情報が同時に遺族等の生存する個人に関する情報でもある場合には、当該生存個人に関する情報として改正法の保護対象となるとする一方で、死者に関する情報の取扱いについて個人情報保護制度とは別の制度として条例を定めることは妨げられていないところである。

この点について、令和4年7月の審議会答申では、区の個人情報保護制度とは別の制度としての条例制定は求めないが、条例の運用と同様に内部管理規定により適切な運用を行うべきであるとした。また、現行条例で運用している「死者の個人情報に関する開示請求の取扱い基準」は、前述の国がガイドライン等で示している死者に関する情報が同時に遺族等の生存する個人に関する情報でもある場合と同じ主旨と考え、今後、現行の開示対象等が区民にとって後退することがないように、死者に関する取扱い基準を内部管理規定として制定することが相当であるとしたものである。

以上のことから、改正法施行時においても、一定程度の死者の情報も生存する個人が開示請求することを可能なものとする現状の運用を継続するため、「死者の情報に関する開示請求基準」を改めて策定するものであ

る。

(2) 主な意見

当該基準の法形式を知りたい。また、今後、当該基準を公表する予定はあるか。

当該基準について、区民意見募集等を行う予定はあるか。

内部基準であったとしても一旦紛争になれば外部基準となり得るため、この点留意願いたい。

(3) 考え方

区が提示した「死者の情報に関する開示請求基準」は、現行の「死者の個人情報に関する開示請求の取扱い基準」を実質的に継続するものであって現行制度を後退させるものではなく、令和4年7月の審議会答申の内容に則ったものであると認められるため、異議はない。

参考1 世田谷区情報公開・個人情報保護審議会小委員会 委員名簿

氏 名	現職等	備 考
さいき ひでのり 齊木 秀憲	国土館大学法学部・ 大学院法学研究科教授	委員長
やまだ けんた 山田 健太	専修大学文学部 ジャーナリズム学科教授	委 員
つちだ しんや 土田 伸也	中央大学法科大学院教授	委 員
たかやま こずえ 高山 梢	弁護士	委 員
やまべ なおよし 山辺 直義	弁護士 システム監査技術者	委 員
なかむら しげみ 中村 重美	世田谷地区労働組合協議会	委 員

(敬称略)

参考2 世田谷区情報公開・個人情報保護審議会小委員会 審議経過

(1) 第1回(令和4年10月26日(水))

- ・条例要配慮個人情報の制定(案)
- ・死者の情報に関する開示請求基準(たたき台)
- ・改正法の安全管理措置に関する基準関係

(2) 第2回(令和4年11月8日(火))

- ・条例要配慮個人情報の制定(案)
- ・死者の情報に関する開示請求基準(案)
- ・個人情報保護管理基準(案)
- ・外部委託等の審査基準(案)
- ・開示請求手続の本人確認書類(案)

資料 2 - 1

個人情報保護条例の審議会諮問事項と改正法に基づく区の対応について

現行条例においては、審議会諮問事項が規定されています。しかしながら、法改正により審議会諮問事項は、許容されていません。区としては、法改正後に法の規定を遵守しつつ適正に個人情報保護を図っていきます。

現行条例の審議会諮問事項	法改正に基づく区の対応
収集禁止事項 (第7条)	改正法の第61条(個人情報の保有の制限等)、第62条(利用目的の明示)、第63条(不適正な利用の禁止)、第64条(適正な取得)に基づき収集の可否等を判断することとします。 国が示しているガイドライン及び事務対応ガイドから該当部分を抜粋(次頁に別紙添付)の内容から『個人情報の保有に関する審査基準』を策定し、所管課が適切にチェックし、総括個人情報保護管理者あて報告することとします。
本人外収集 (第8条・第6条)	
外部委託 (第12条)	○条例施行規則に基づく個人情報保護管理基準に基づき『外部委託の審査基準』を策定し、所管課が適切にチェックし、総括個人情報保護管理者あて報告することとします。
目的外利用 (第15条・第14条)	○条例施行規則に基づく個人情報保護管理基準に基づき『目的外利用の審査基準』を策定し、所管課が適切にチェックし、総括個人情報保護管理者あて報告することとします。
外部提供 (第16条・第14条)	○条例施行規則に基づく個人情報保護管理基準に基づき『外部提供の審査基準』を策定し、所管課が適切にチェックし、総括個人情報保護管理者あて報告することとします。
電子計算機への記録 (第17条)	○条例施行規則に基づく個人情報保護管理基準に基づき『オンライン結合・システム導入の審査基準』を策定し、所管課が適切にチェックし、総括個人情報保護管理者あて報告することとします。
回線結合 (第18条)	

改正法第61条（個人情報の保有の制限等）第62条（利用目的の明示）
第63条（不適正な利用の禁止）第64条（適正な取得）にかかる
事務対応ガイド及びガイドライン

4 個人情報等の取扱い

4-1 保有に関する制限（法第61条）

法第61条

- 1 行政機関等は、個人情報を保有するに当たっては、法令（条例を含む。第66条第2項第3号及び第4号、第69条第2項第2号及び第3号並びに第4節において同じ。）の定める所掌事務又は業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない。
- 2 行政機関等は、前項の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。

行政機関等は、条例を含む法令で当該行政機関等が行うことができるとされている具体的な所掌事務又は業務の遂行に必要な限度でのみ、個人情報を保有することができる。また、以上に加えて、個人情報を保有するに当たっては、利用目的をできる限り特定しなければならない。

【ガイドライン】5-1 保有に関する制限

行政機関等においては、行政サービスの提供等のために個人情報を保有する必要がある一方で、不必要な個人情報の保有は、安全管理上問題であるのみならず、場合によっては誤った利用等がなされるおそれもある。そのため、法においては、行政機関等が個人情報を保有することができる場合について規定するとともに、個人情報を保有するときは利用目的を特定すること等を求めている。

行政機関等は、法令の定めに従い適法に行う事務又は業務を遂行するため必要な場合に限り、個人情報を保有することができる（法第61条第1項）。

事務又は業務については、行政機関等が事実上行っているというだけでなく、法令上の根拠が必要であり、行政機関等の設置の根拠となる法令において「所掌事務」等を定める条文に列挙されている事務又は業務のほか、「権限」を定める条文上で規定されている事務又は業務や、作用法上規定されている事務又は業務が含まれる。地方公共団体においては、地方自治法第2条第2項に規定する「地域における事務」もこれに含まれる。

なお、所掌事務又は業務の根拠となる法第61条第1項の「法令」には、条例が含まれる

ほか、規則等の地方公共団体が法令に基づき定める法規が含まれる。

また、同項の規定により、行政機関等は、個人情報の利用目的について、当該個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ具体的かつ個別的に特定しなければならない。この際、行政機関等の恣意的な判断により利用目的の特定の程度を弱めることは許容されず、具体的な利用行為が当該利用目的の範囲内であるか否か、合理的かつ明確に判断することができるものでなければならない。

さらに、法第61条第2項の規定により、行政機関等は、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。そのため、個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならない。

(1) 個人情報を保有する(第61条第1項)

- 「保有個人情報」とは、行政機関等の職員が職務上作成し、又は取得した個人情報であって、当該行政機関等の職員が組織的に利用するものとして、当該行政機関等が保有しているもののうち、行政文書又は法人文書に記録されているものをいう。
- 「行政機関等の職員が職務上作成し、又は取得した」とは、行政機関等の職員が当該職員に割り当てられた仕事を遂行する立場で、すなわち公的立場において作成し、又は取得したことをいう。
- 「組織的に利用する」とは、作成又は取得に関与した職員個人の段階のものではなく、組織の業務上必要な情報として利用されることをいう。
- 「行政機関等が保有している」とは、行政機関情報公開法における行政文書の保有の概念と同様である。
- すなわち、職務上作成し、又は取得した個人情報について事実上支配している(当該個人情報の利用、提供、廃棄等の取扱いについて判断する権限を有している)状態をいう。
- したがって、例えば、行政機関等が個人情報をクラウドサービス上で利用しており、物理的には当該個人情報が当該クラウドサービスを提供する事業者の管理するサーバ上に保管されている場合であっても、これに含まれ得る。

(2) 法令の定める所掌事務又は業務を遂行するため必要な場合に限り(第61条第1項)

- 「法令の定める所掌事務又は業務を遂行するため必要な場合に限り」とは、個人情報の保有が、これらの所掌事務又は業務のうち、当該個人情報を保有することによって遂行しようとする具体的な事務又は業務の遂行に必要な場合に限り許容されることを意味する。

(3) その利用目的をできる限り特定しなければならない(第61条第1項)

- 個人情報が無限定に取り扱われ、個人が不測の権利利益侵害を被ることを未然に防止するためには、まず、個人情報の利用目的が明確にされ、以後、その利用目的に沿って適切に取り扱われることが必要である。
- 「利用目的」は、保有から利用及び提供に至る個人情報の取扱いの範囲に係る重要な要素である。
- なお、特定した利用目的については、保有個人情報の開示を行う場合に開示請求者に対して通知しなければならないことから（法第82条第1項）、内部において適切に整理・管理する必要がある。そのため、利用目的の特定の方法として、利用目的について内部的に整理したものを文書化しておくといった対応などが考えられる。

(4) 行政機関等が個人情報を保有するに当たっては、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない(第61条第2項)

- 利用目的の達成に不必要な個人情報の保有は、安全管理上問題であるのみならず、場合によっては誤った利用等がなされるおそれもある。したがって、個人の権利利益を保護する観点から、個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならないこととしている。

【ガイドライン】 5 1 保有に関する制限(一部抜粋)

行政機関等は、個人情報の利用目的について、当該個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ具体的かつ個別的に特定しなければならない。この際、行政機関等の恣意的な判断により利用目的の特定の程度を弱めることは許容されず、具体的な利用行為が当該利用目的の範囲内であるか否か、合理的かつ明確に判断することができるものでなければならない。

さらに、法第61条第2項の規定により、行政機関等は、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。そのため、個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならない。

【ガイドライン】 5 2 取得及び利用の際の遵守事項

行政機関等は、個人情報を適正に取得し、その利用目的の範囲内で取り扱わなければならない。他方で、新たな行政サービスの展開に対応する必要性等から、利用目的を変更せざるを得ない場合が生じることは一般に想定し得るところである。法第1条にもあるとおり、法は、個人の権利利益を保護することを目的としつつも、行政機関等の事務及び事業の適正かつ円滑な運営を図ることに留意して、行政機関等が個人情報を取得及び利用の際の遵守事項について規定している。

4-2 取得及び利用の際の遵守事項

4-2-1 利用目的の変更（法第61条第3項）

法第61条（第3項）

3 行政機関等は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

新たな行政サービスの展開に対応する必要性等から、利用目的を変更せざるを得ない場合が生じることは一般に想定し得るところであり、行政機関等の事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護するという法の目的に照らせば、利用目的に一定の柔軟性を持たせることが適当である。

しかしながら、いったん特定された利用目的が無限定に変更されることになれば、利用目的を特定した実質的意味は失われることから、本項では、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲に限り、利用目的を変更することができる。

【ガイドライン】 5 2 1 利用目的の変更

行政機関等が個人情報利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えてはならない（法第61条第3項）。

当初の利用目的に照らして、変更後の利用目的を想定することが困難であるような場合には、「変更前の利用目的と相当の関連性を有する」とは認められない。

また、「合理的に認められる」とは、社会通念上妥当であると客観的に認識されるとの趣旨であり、行政機関等の恣意的な判断による変更を認めるものではない。

（1）相当の関連性を有する

○「相当の関連性を有する」とは、当初の利用目的からみて、変更後の利用目的を想定することが困難でない程度の関連性を有することをいう。

（2）合理的に認められる

○「合理的に認められる」とは、社会通念上妥当であると客観的に認識されるとの趣旨であり、行政機関等の恣意的な判断による変更を認めるものではない。

○例えば、許認可の審査のために提出された申請書を当該許認可に係る統計作成の目的で利用する場合には、「相当の関連性を有すると合理的に認められる範囲」に該当する。

(3) 利用目的以外の目的のための利用及び提供の制限との関係

- 利用目的以外の目的のための利用及び提供が恒常的に行われる場合は、本項に基づく利用目的の変更に該当し、臨時的に行われる場合は、法第 69 条第 2 項の規定に基づく利用目的以外の目的のための利用及び提供に該当する。
- なお、利用目的以外の目的のための利用及び提供を恒常的に行うことを個人情報の取得前から予定している場合は、そのような利用及び提供が可能となるように利用目的を設定しておく必要がある。

4-2-2 本人から書面により取得する際の利用目的の明示（法第 62 条）

法第 62 条

行政機関等は、本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときは、次に掲げる場合を除き、あらかじめ、本人に対し、その利用目的を明示しなければならない。

- (1) 人の生命、身体又は財産の保護のために緊急に必要があるとき。
- (2) 利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき。
- (3) 利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき。
- (4) 取得の状況からみて利用目的が明らかであると認められるとき。

(1) 利用目的の明示

- 行政機関等は、本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときは、法第 62 条各号に掲げる場合を除き、あらかじめ、本人に対し、その利用目的を明示しなければならない。

【ガイドライン】 5 2 2 本人から書面により取得する際の利用目的の明示（一部抜粋）

行政機関等は、本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときには、次のいずれかに該当する場合を除き、本人が認識することができる適切な方法により、本人に対し、利用目的をあらかじめ明示しなければならない（法第62条）。

- (1) 人の生命、身体又は財産の保護のために緊急に必要があるとき（同条第1号）。
- (2) 利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき（同条第2号）。

(3) 利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき（同条第3号）。

(4) 取得の状況からみて利用目的が明らかであると認められるとき（同条第4号）。

○「本人から直接書面（電子的記録を含む。）に記録された当該本人の個人情報を取得するとき」について、法が定める個人情報の取扱い等に係る規律は行政文書等に記録されていることを前提とする保有個人情報に対して課せられているところであり、申請書やアンケート調査票等、本人が書面に記載等することで提出するものは、その多くが保有個人情報として保有され、その後の行政機関等における事務や事業の運営の基礎資料として利用されることになると考えられることから、本人から直接書面に記載された当該本人の個人情報を取得する場合は、特に利用目的を明示することを定めたものである。

○なお、「電磁的記録を含む」こととしたのは、行政のデジタル化に伴い、オンラインによる申請等も一般化しつつあることから、このような方法を介して取得する場合も含む趣旨である。

○「あらかじめ、本人に対し、その利用目的を明示しなければならない」について、利用目的の明示の方法としては、申請書等の様式にあらかじめ記載しておくなどの方法のほか、窓口における掲示や口頭による方法も考えられるが、本人が利用目的を認識することができるよう、適切な方法により行うことが必要である（ ）。（ ）ホームページにおいてあらかじめ必要な情報を掲載しておく場合も考え得るが、この場合には、本人が送信ボタン等をクリックする前等にその利用目的（利用目的の内容が示された画面に 1 回程度の操作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目に留まるようその配置に留意することが望ましい。

○他方、行政機関等に対して一方的に個人情報をその内容に含む書面が送りつけられてきたような場合には、そもそも「あらかじめ」利用目的を明示することが不可能であり、そのような場合についてまで「あらかじめ」利用目的を明示しなければならない義務を課すものではない。

【ガイドライン】 5 2 2 本人から書面により取得する際の利用目的の明示（一部抜粋）

なお、行政機関等に対して個人情報をその内容に含む書面が一方的に送りつけられてきたような場合には、そもそも「あらかじめ」利用目的を明示することが不可能であり、そのような場合については、同条の規定の適用を受けない。

(2) 利用目的の明示の適用除外

○利用目的を明示することにより他の権利利益を損なうおそれがある場合等、利用

目的の明示を義務付けることが適当でない場合や、利用目的が明らかである場合にまで、一律にあらかじめ利用目的を明示することは合理的でなく、法第 62 条第 1 号から第 4 号まではこれらの適用除外について定めている。

人の生命、身体又は財産の保護のために緊急に必要があるとき（第 1 号）

- ・本人又は第三者の生命、身体又は財産を保護するための個人情報の取得であって、利用目的を明示する時間的余裕がない場合に、適用を除外したものである。

利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき（第 2 号）

- ・利用目的を明示することにより、本人又は第三者の不利益になる場合や、結果として本人又は第三者に損害を与えるおそれがある場合にまで利用目的を明示する義務を課すことは適当でないことから、適用を除外したものである。

利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき（第 3 号）

- ・「国の機関」には、行政機関のほか、裁判所及び国会の機関も含まれる。
- ・国の機関、独立行政法人等、地方公共団体又は地方独立行政法人（以下 4-2-2（本人から書面により取得する際の利用目的の明示）において「国の機関等」という。）の事務又は事業の適正な遂行に支障を及ぼすおそれがある場合には公共の利益が損なわれるおそれがあり、このような場合にまで利用目的を明示する義務を課すことは適当でないことから、適用除外としたものである。
- ・国の機関等が行う事務又は事業の内容は多様であるため、「事務又は事業の適正な遂行に支障を及ぼすおそれ」があるかどうかについて一般的な基準を定めることは困難であり、社会通念により個別具体的に判断せざるを得ないが、例えば、利用目的を明示することにより、以後の個人情報の収集が困難になる場合、被疑者の逃亡、証拠隠滅につながる場合、適正な判断・評価に支障を及ぼす場合等はこれに該当すると考えられる。

取得の状況からみて利用目的が明らかであると認められるとき（第 4 号）

- ・個人情報取得される状況からみて利用目的が明らかである場合は、本人が利用目的を確認するための措置をあえて講ずる必要性が認められないと考えられることから、適用除外とされている。
- ・例えば、特定の許認可申請を行うため本人が自己の個人情報を記載した申請書を行政機関に提出する場合であって、行政機関が当該許認可申請の事務処理のみに当該個人情報を利用する場合等が考えられる。

4-2-3 不適正な利用・取得の禁止（法第 63 条及び第 64 条）

4-2-3-1 不適正な利用の禁止（法第 63 条）

法第 63 条

行政機関の長（第 2 条第 8 項第 4 号及び第 5 号の政令で定める機関にあっては、その機関ごとに政令で定める者をいう。以下この章及び第 174 条において同じ。）地方公共団体の機関、独立行政法人等及び地方独立行政法人（以下この章及び次章において「行政機関の長等」という。）は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

行政機関の長等は、個人情報の適正な取扱いに対する国民等の信頼確保の観点から、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

【ガイドライン】 5 2 3 不適正な利用及び取得の禁止

行政機関の長等は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならず（法第 63 条）、また、偽りその他不正の手段により個人情報を取得してはならない（法第 64 条）。

「違法又は不当な行為」とは、法その他の法令に違反する行為及び直ちに違法とはいえないものの、法その他の法令の制度趣旨又は公序良俗に反する等、社会通念上適正とは認められない行為をいう。

「おそれ」の有無は、行政機関の長等による個人情報の利用が、違法又は不当な行為を助長し、又は誘発することについて、社会通念上蓋然性が認められるか否かにより判断される。

違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用する具体例としては、正当な理由なく本人に対する違法な差別的取扱いを行うために個人情報を利用する場合等が考えられる。

また、不正の手段により個人情報を取得する具体例としては、行政サービスの見返りとして本来は提供する必要のない個人情報を提供しよう強要し、これを取得する場合等が考えられる。

（1）違法又は不当な行為

○「違法又は不当な行為」とは、法（個人情報の保護に関する法律）その他の法令に違反する行為や、直ちに違法とはいえないものの、法（個人情報の保護に関する法律）その他の法令の制度趣旨又は公序良俗に反する行為等、社会通念上適正とは認められない行為をいう。

(2) おそれの有無

- 「おそれ」の有無は、行政機関の長等による個人情報の利用が、違法又は不当な行為を助長し、又は誘発することについて、社会通念上蓋然性が認められるか否かにより判断される。
- この判断に当たっては、個人情報の利用方法等の客観的な事情に加えて、個人情報の利用時点における行政機関等の認識及び予見可能性も踏まえる必要がある。
- 例えば、行政機関等が第三者に個人情報を提供した場合において、当該第三者が当該個人情報を違法な行為に用いた場合であっても、当該第三者が当該個人情報の取得目的を偽っていた等、当該個人情報の提供の時点において、提供した個人情報が違法に利用されることについて、当該行政機関等が一般的な注意力をもってしても予見することができない状況であった場合には、「おそれ」は認められないと解される。

4-2-3-2 不適正な取得の禁止（法第 64 条）

法第 64 条

行政機関の長等は、偽りその他不正の手段により個人情報を取得してはならない。

行政機関の長等は、個人情報の適正な取扱いに対する国民等の信頼確保の観点から、個人情報を適正に取得しなければならない。なお、例えば、個人情報を含む情報がインターネット等により公にされている場合であって、単にこれを閲覧するにすぎず、転記等を行わない場合は、個人情報を取得しているとは解されない。

個人情報保有に関する審査基準（別票）（案）

個人情報を保有する前に、以下のすべての項目に適合するか確認し、「適合」する場合、各チェック欄に 印または設問に従い記載をしてください。不明な点があれば、区政情報課区政情報係あてご相談ください。確認が終わったら、個人情報の保有に関する審査基準に添付してください。

No.	確認項目	チェック欄
1	<p>事務又は業務については、区が事実上行っているというだけでなく、法令上の根拠が必要であるが、根拠規定は明確になっているか。 （ 根拠となる法第61条第1項の「法令」には、条例が含まれるほか、規則等の区が法令に基づき定める法規が含まれる。）</p>	
2	<p>個人情報の利用目的について、当該個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ具体的かつ個別的に特定しなければならないとのことに適合するか。 （ 行政機関等の恣意的な判断により利用目的の特定の程度を弱めることは許容されず、具体的な利用行為が当該利用目的の範囲内であるか否か、合理的かつ明確に判断することができるものでなければならない。）</p>	
3	<p>個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならないとのことに適合するか。 （ 特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。）</p>	
4	<p>本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときには、次のいずれかに該当する場合を除き、本人が認識することができる適切な方法により、本人に対し、利用目的をあらかじめ明示しなければならないとの規定において、該当する場合は（1）～（4）の番号を右欄に記載のこと。それ以外の場合は、「該当なし」と記載し、次の5において回答のこと。</p> <p>（1）人の生命、身体又は財産の保護のために緊急に必要があるとき（第1号）。 （2）利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき（第2号）。 （3）利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき（第3号）。 （4）取得の状況からみて利用目的が明らかであると認められるとき（第4号）。</p>	

No.	確 認 項 目	チェック欄
5	<p>本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報 を取得するときには、本人が認識することができる適切な方法により、本人に 対し、利用目的をあらかじめ明示しなければならないことに適合するか。 （ 個人情報をその内容に含む書面が一方的に送りつけられてきたような場 合には、そもそも「あらかじめ」利用目的を明示することが不可能であり、そ のような場合は、規定の適用を受けない。）</p>	
6	<p>違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情 報を利用してはならず、また、偽りその他不正の手段により個人情報を取得し てはならないとすることを遵守できるか。 （ 個人情報を含む情報がインターネット等により公にされている場合であ って、単にこれを閲覧するにすぎず、転記等を行わない場合は、個人情報を取 得しているとは解されない。）</p>	
7	<p>【利用目的を変更するときのみに回答】 行政機関等が個人情報の利用目的を変更する場合には、変更前の利用目的と 相当の関連性を有すると合理的に認められる範囲を超えてはならないことに 適合しているか。 （ 「合理的に認められる」とは、社会通念上妥当であると客観的に認識され るとの趣旨であり、行政機関等の恣意的な判断による変更を認めるものではな い。）</p>	

外部委託の審査基準（別票A）【マニュアル処理による委託】 （案）

必ず契約締結前に、契約予定の事業者に対して、以下のすべての項目に適合するか確認を求め、「適合」する場合、各チェック欄に 印をしてください。確認が終わったら、外部委託の審査基準に添付してください。不明な点があれば、区政情報課区政情報係あてご相談ください。

No.	確認項目	チェック欄
1	（秘密保持義務） 受託者は、この契約の履行により直接又は間接に知り得た個人情報を、第三者に漏らしてはならない。また、契約期間満了後も同様とする。	
2	（書面主義の原則） 受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。	
3	（管理体制等の通知） 受託者は、この契約の締結後直ちに、以下の文書を委託者に提出しなければならない。 （1）個人情報保護に関する社内規程又は基準 （2）以下の内容を含む従事者名簿 個人情報を取り扱う者の氏名、責任及び役割 委託業務において個人情報の授受に携わる者の氏名及び業務執行場所 緊急連絡先一覧 （3）委託業務に係る実施スケジュールを明記した文書	
4	（再委託の禁止） 受託者は、この契約による業務を第三者に再委託してはならない。ただし、当該業務の全部又は一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容を委託者に通知し、委託者の承諾を得なければならない。また、再受託者（委託先の子会社（会社法（平成17年法律第86号）第2条第1項第3号に規定する子会社をいう。）である場合も含む。）にも、この契約を遵守させなければならない。	
5	（目的外使用及び外部提供の禁止） 受託者は、個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。	
6	（複写及び複製の禁止） 受託者は、個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。	
7	委託者の許可を受けて複写又は複製したときは、委託業務の終了後直ちに当該複写物又は複製物を利用できないよう処分又は委託者へ提出しなければならない。	

8	<p>(安全管理措置の実施)</p> <p>受託者は、委託業務において、委託者に提出した個人情報保護に関する社内規程又は基準を遵守しなければならない。</p>	
9	<p>受託者は、従事者に対して、個人情報に関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。</p>	
10	<p>受託者は、個人情報の授受、保管及び管理について、善良な管理者の注意をもって当たり、個人情報の漏えい、滅失、毀損等(以下「漏えい等」という。)の事故を防止しなければならない。</p>	
11	<p>(委託終了時における個人情報の消去及び媒体の返却)</p> <p>受託者は、委託業務が終了したときは、速やかに、委託業務に使用した個人情報の消去及び個人情報記録された媒体の返却をしなければならない。</p>	
12	<p>(委託業務の報告)</p> <p>受託者は、委託者に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。</p>	
13	<p>(監査、施設への立入検査の受入れ)</p> <p>受託者は、委託者が必要とする場合、監査又は検査を受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。</p>	
14	<p>受託者は、委託者が必要とする場合は、業務執行場所へ委託者の職員の立入りを認めるものとする。</p>	
15	<p>(個人情報の漏えい等の対応)</p> <p>受託者は、個人情報の漏えい等が生じたとき、又は漏えい等が生じたおそれがあるときには直ちに委託者に対して連絡するとともに、遅滞なくその状況について書面をもって委託者に報告し、委託者の指示に従わなければならない。</p>	
16	<p>(契約解除及び損害賠償)</p> <p>受託者が、個人情報の取扱いについて法令及び本特記事項に違反した場合、委託者は契約解除を申し出ることができる。また、受託者が、個人情報の取扱いにつき法令及び本特記事項に違反したことにより、委託者に損害が生じた場合には、これを賠償するものとする。</p>	
17	<p>【契約書を交わさない場合のみ】</p> <p>当該業務は日本国の法令に準拠し、当該業務に係る訴訟については、日本国の裁判所をもって合意による専属的管轄裁判所とする。</p>	

外部委託の審査基準（別票B）【電算処理による委託】 （案）

必ず契約締結前に、以下の項目のうち、電算処理の類型に応じて契約条件とするべきすべての項目について、契約予定の事業者に対して確認を求め、「適合」する場合、各チェック欄に印をしてください。契約条件にあてはまらない項目には「-」と記載してください。確認が終わったら、外部委託の審査基準に添付してください。不明な点があれば、区政情報課区政情報係あてご相談ください。

No.	確 認 項 目	チェック欄
1	<p>（秘密保持義務）</p> <p>受託者は、当該委託契約（業務内容に保守委託を伴う賃貸借契約等を含む。以下同じ。）に係る電算処理業務（以下「委託業務」という。）により知り得た個人情報その他の情報（以下「情報」という。）を、いかなる理由があっても第三者に漏らしてはならず、この旨を委託業務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。また、契約期間満了後も、同様とする。</p>	
2	<p>（書面主義の原則）</p> <p>受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。</p>	
3	<p>（管理体制等の通知）</p> <p>受託者は、当該委託契約の締結後直ちに、以下の文書を区に提出しなければならない。提出後に内容の変更があった場合も、同様とする。</p> <p>(1) 情報セキュリティ及び個人情報保護に関する社内規程又は基準</p> <p>(2) 以下の内容を含む従事者名簿 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所 委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所 委託業務に関する緊急時連絡先一覧</p> <p>(3) 委託業務に係る実施スケジュールを明記した文書</p> <p>(4) 委託業務において使用する情報システムのネットワーク構成図(特定個人情報ファイル(コンピュータ等で検索することができるように体系的に構成した情報の集合体であって、個人番号をその内容に含むもの。以下同じ。))を取り扱う場合のみ。第23項の事項を証するもの。)</p> <p>(5) 委託業務において使用する情報システムのセキュリティ仕様書(特定個人情報ファイルを取り扱う場合のみ。第24項の事項を証するもの。)</p> <p>(6) クラウドサービス(有料、無料に関わらず、民間事業者等がインターネット上で提供する情報処理サービスで、約款への同意及び簡易なアカウ</p>	

	<p>ントの登録等により当該機能が利用可能となるサービスのこと。以下同じ。) 利用に係るリスク対策文書(委託業務においてクラウドサービスを利用する場合のみ。第25項の事項を証するもの。)</p>	
4	<p>(再委託の禁止)</p> <p>受託者は、委託業務の全部又は一部を、他の者に再委託してはならない。ただし、附属業務でやむを得ず再委託する必要があるときは、受託者は、再受託者(委託先の子会社(会社法(平成17年法律第86号)第2条第1項第3号に規定する子会社をいう。))である場合も含む。以下同じ。)に当該委託契約及び本特記事項を遵守させ、かつ、再受託者にかかる再委託の内容及び第3項に規定する事項を、区に事前に書面をもって通知し、その承認を得なければならない。</p> <p>再受託者も、委託業務の全部又は一部を、他の者に更に再委託してはならない。附属業務でやむを得ず更に再委託する必要があるときは、再委託と同様の条件と手続きにより、区の承認を得なければならない。更に再委託が繰り返される場合も同様とする。</p>	
5	<p>(目的外使用等及び複写等の禁止)</p> <p>受託者は、委託業務で取り扱う情報を委託業務の目的以外に使用してはならない。また、第三者に提供してはならない。</p>	
6	<p>受託者は、区が委託業務での使用を目的として受託者に提供し、又は貸与する情報及び情報資産(世田谷区電子計算組織の運営に関する規則(平成16年世田谷区規則第47号)第2条第9号に規定する情報資産をいう。以下同じ。)を、委託業務以外の目的に使用してはならない。</p>	
7	<p>受託者は、委託業務で取り扱う情報及び情報資産について、業務上必要なバックアップを取得する場合を除き、区の承認を得ずに複写してはならない。委託業務を実施する上でやむを得ず複写するときは、あらかじめ区に通知し、その承認を得なければならない。この場合において、委託業務の終了後、受託者は、直ちに複写した情報及び情報資産を消去又は廃棄し、使用できない状態にするとともに、情報及び情報資産を消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。</p>	
8	<p>受託者は、区の事前の承諾なく、委託業務で取り扱う情報及び情報資産を区の事業所または受託者の事業所から持ち出してはならない。</p>	
9	<p>(物的セキュリティ対策)</p> <p>受託者は、委託業務に使用する情報システムに係る装置の取付けを行う場合は、できる限り、火災、水害、埃、振動、温度、湿度等の影響を受けない場所に設置するものとし、施錠等容易に取り外すことができないよう必要な措置を講じなければならない。</p>	

10	受託者は、委託業務に係る区が運用する情報システムのサーバ等を区庁舎外に設置する場合は、区の承認を得なければならない。また、定期的に当該サーバ等への情報セキュリティ対策状況について確認するとともに、区から要請があった場合は、その結果を区に報告しなければならない。	
11	受託者は、その従事者に名札等の着用及び身分証明書等の携帯を義務付け、区の情報システム室その他の区の管理区域に立ち入る場合において区から求められたときは、身分証明書等を提示するよう指導しなければならない。	
12	受託者は、委託業務で使用するパソコン等の盗難を防止するため、当該パソコン等をセキュリティワイヤーで固定し、又は従事者が業務執行場所を離れる間において施錠可能なロッカー等に収納させるなどの措置を講じなければならない。	
13	(人的セキュリティ対策) 受託者は、委託業務において、区に提出した情報セキュリティ及び個人情報保護に関する社内規程又は基準を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに区に報告し、代替策について協議しなければならない。	
14	受託者は、情報及び情報資産を適切に保管するものとし、パソコン等により情報及び情報資産を使用する場合は、第三者に使用され、又は閲覧されることがないように、離席時にパスワードロック又はログオフ等を行わなければならない。	
15	受託者は、従事者に情報システムの保守又は運用業務に関し、次の事項を遵守させなければならない。 (1) 自己が利用している ID は、他人に利用させないこと (ID の共用を指定されている場合は除く。) (2) 共用 ID を利用する場合は、共用 ID の利用者以外の者に利用させないこと。 (3) パスワードを秘密にし、パスワードの照会等には一切応じないこと (パスワード発行業務を除く。) (4) パスワードのメモの不用意な作成等により、パスワード流出の機会を作らないこと。 (5) パスワードは、十分な長さとし、想像し難い文字列とすること。 (6) 複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しないこと。 (7) パソコン等のパスワードの記憶機能を利用しないこと。 (8) 社員間でパスワードを共有しないこと (ID の共用を指定されている場合を除く。)	
16	受託者は、従事者に対して、情報セキュリティに関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。	

17	<p>(技術的及び運用におけるセキュリティ対策)</p> <p>受託者は、情報システムの保守又は運用業務を遂行するに当たり、情報システムの変更記録、作業日時及び実施者を記録するとともに、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。</p>	
18	<p>受託者は、アクセスログ等を取得するサーバについて、正確な時刻設定を行わなければならない。自動的にサーバ間の時刻同期が可能な場合は、その措置を講じなければならない。</p>	
19	<p>受託者は、情報システム等に記録された重要性の高い情報について、定期的にバックアップを取得しなければならない。また、バックアップの取得前にその手法を区に通知し、承認を得なければならない。</p>	
20	<p>受託者は、情報システムの開発及び導入に当たり、開発及び導入前に区と協議の上、情報セキュリティに係る検証事項を定め、検証を実施しなければならない。</p>	
21	<p>受託者は、委託業務に使用する情報システムがネットワークに接続されている場合は、不正アクセスを防ぐため、常にセキュリティホールの発見に努め、メーカー等からのセキュリティ修正プログラムの提供があり次第、情報システムへの影響を確認し、区と協議の上、修正プログラムを適用しなければならない。また、ウィルスチェックを行い、ウィルスの情報システムへの侵入及び拡散を防止しなければならない。</p>	
22	<p>受託者は、情報システムを開発する場合は、システム開発及びテスト環境と、本番運用環境を分離しなければならない。</p>	
23	<p>受託者は、委託業務において特定個人情報ファイルを取り扱う場合は、当該特定個人情報ファイルをインターネットから物理的又は論理的に分離された環境にて取り扱わなければならない。</p>	
24	<p>受託者は、委託業務に使用する情報システムにおいて特定個人情報ファイルを取り扱う場合は、定期に及び必要に応じ随時に当該情報システムのログ等の分析を行うなど不正アクセス等を検知する仕組みを講じるとともに、当該情報システムの不正な構成変更(許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等)を防止するために必要な措置を講じなければならない。</p>	
25	<p>受託者は、委託業務においてクラウドサービスを利用する場合は、当該クラウドサービスの利用に伴い想定される情報セキュリティ上のリスクを回避するために必要な措置を講じなければならない。(例:当該クラウドサービス提供事業者が公表している情報セキュリティ対策内容の確認、受託者が従業員に付与するクラウドサービス用IDの適切な付与管理、クラウドサービス上に記録した情報が第三者に提供される場合についての確認、サービス利用終了時の</p>	

	データの取扱い条件の確認、等)	
26	<p>(データのセキュリティ対策)</p> <p>受託者は、委託業務に関し、区より情報及び情報資産を受領した場合は、預かり証を区に対して交付しなければならない。また、当該情報及び情報資産を適切に管理するため、情報及び情報資産の受領日時、受領者名、受領した情報及び情報資産の種類等の記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を区に提示しなければならない。</p>	
27	<p>受託者は、委託業務に係る重要度の高い情報及び情報資産を運搬する場合は、可能な限り暗号化、パスワード設定等の保護対策を行い、鍵付きのケース等に格納する等、情報及び情報資産の滅失や不正利用を防止するための処置を講じなければならない。また、重要度の高い情報を電子メール等で送受信する場合は、暗号化、パスワード設定等の保護対策を行わなければならない。</p>	
28	<p>受託者は、委託業務で取り扱う情報及び情報資産を施錠可能な金庫、ロッカー等に適切に保管する等善良な管理者の注意をもって当たり、情報及び情報資産の取扱いには十分注意し、情報及び情報資産の滅失、毀損及び漏えい等の防止に努めなければならない。</p>	
29	<p>受託者は、委託業務が終了したときは、区より受領した情報及び情報資産を速やかに区に返却しなければならない。また、返却が不可能な情報及び情報資産は、区の上記のとおり、バックアップデータを含め、情報及び情報資産を使用できないように処置した上で消去又は廃棄し、日時、担当者及び処理内容を区に報告しなければならない。</p>	
30	<p>受託者は、情報資産の作成業務を終了したときは、直ちに当該情報資産を区があらかじめ指定した職員に引き渡さなければならない。</p>	
31	<p>(電算処理機器の廃棄)</p> <p>受託者は、委託業務で使用しているサーバ、パソコン等の機器(以下これらを「電算処理機器」という。)を廃棄する場合は、事前に当該電算処理機器に保存されている情報及び情報資産を消去、復元できない状態にした上で廃棄しなければならない。</p>	
32	<p>(委託業務の報告)</p> <p>受託者は、区に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。</p>	
33	<p>(監査、施設への立入検査の受入れ)</p> <p>受託者は、情報及び情報資産の情報セキュリティ管理状況について、区の求めに応じて報告するものとする。また、区が必要に応じて監査又は検査を実施する場合は受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。</p>	

34	<p>受託者は、区が必要とする場合は、業務執行場所へ区の職員の立入りを認めるものとする。</p>	
35	<p>(緊急時の対応) 受託者は、委託業務において、業務上のトラブル、災害、事故、電算処理機器の不良、故障及び破損等が発生した場合は、直ちに区にその状況について報告し、区の指示に従わなければならない。</p>	
36	<p>受託者は、委託業務について次に掲げる事象が発生した又は発生したおそれがある場合は、直ちに、区にその状況を具体的に報告しなければならない。</p> <ul style="list-style-type: none"> (1) 情報及び情報資産の滅失 (2) 情報及び情報資産の毀損 (3) 情報の漏えい (4) 不正アクセス (5) 情報セキュリティポリシーの違反 (6) 前各号に掲げるもののほか、情報セキュリティに悪影響を及ぼす事象 	
37	<p>(サービスレベルの保証) 受託者は、委託業務のサービスレベルについて、事前に区と合意している場合は、そのサービスレベルを保証するものとする。</p>	
38	<p>(契約解除及び損害賠償) 受託者が、本特記事項に違反した場合、区は契約解除を申し出ることができる。また、受託者は、本特記事項に違反し、又は本特記事項を履行しなかったことにより、区に損害が生じた場合には、区に対しこれを賠償するものとする。</p>	

目的外利用の審査基準（別票）（案）

実施機関内部から利用の申し出があった場合、法第69条の規定に基づき、利用の可否を検討します。

・法第69条第1項

「法令」に基づく利用

・根拠法令：

第1項の「法令」は法律、政令、府省令等。訓令や通達は含まず、条例も基本的には含まれない。

・法第69条第2項

「本人又は第三者の権利利益を不当に侵害するおそれがない」

かつ 「以下のいずれか」に該当する

本人の同意がある（第2項第1号）

業務の遂行に必要な限度で利用することに相当の理由がある（第2項第2号）

・相当の理由：

【相当の理由】

実施機関の恣意的な判断を許容するものではなく、社会通念上、客観的にみて合理的な理由といえるものである必要がある。

< 参考 >

第69条 行政機関の長等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報から自ら利用し、又は提供してはならない。

2 前項の規定にかかわらず、行政機関の長等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報から自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

(1) 本人の同意があるとき、又は本人に提供するとき。

(2) 行政機関等が法令の定める所掌事務又は業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当の理由があるとき。

(以下略)

外部提供の審査基準（別票）（案）

他の実施機関、外部から提供の申し出があった場合、法第69条の規定に基づき、提供の可否を検討します。

・法第69条第1項

「法令」に基づく提供

根拠法令：

第1項の「法令」は法律、政令、府省令等。訓令や通達は含まず、条例も基本的には含まれない。

例)・刑事訴訟法第197条第2項（捜査に必要な取調べ）

同法第507条（公務所等への照会）

・弁護士法第23条の2（報告の請求）

・民事訴訟法第186条（調査の囑託）、第223条第1項（文書提出命令等）及び第226条（文書送付の囑託）

・法第69条第2項

「本人又は第三者の権利利益を不当に侵害するおそれがない」

かつ 「以下のいずれか」に該当する

本人の同意がある 又は 本人に提供する（第2項第1号）

他の実施機関、国、独立行政法人、他の自治体、地方独立行政法人が行う業務において必要な限度において利用することに相当の理由がある（第2項第3号）

・相当の理由：

専ら統計の作成又は学術研究の目的のために利用されるものとして提供する（第2項第4号）

提供することが明らかに本人の利益になる（第2項第4号）

提供することについて特別の理由がある（第2項第4号）

・特別の理由：

* 提供前に区政情報課区政情報係へ連絡

【相当の理由】

実施機関の恣意的な判断を許容するものではなく、社会通念上、客観的にみて合理的な理由といえるものである必要がある。

< 続く >

【特別の理由】

「相当の理由」よりも更に厳格な理由が必要。

具体的には、行政機関等に提供する場合と同程度の公益性があること、提供を受ける側が自ら当該保有個人情報に相当する個人情報を取得することが著しく困難であること、提供を受ける側の事務が緊急を要すること、当該保有個人情報の提供を受けなければ提供を受ける側の事務の目的を達成することが困難であること等

< 参考 >

第69条 行政機関の長等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

2 前項の規定にかかわらず、行政機関の長等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

(1) 本人の同意があるとき、又は本人に提供するとき。

(2) (略)

(3) 他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当の理由があるとき。

(4) 前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由があるとき。

オンライン結合・システム導入における審査基準（案）

個人情報を利用しオンライン結合による民間サービスの利用、または、システム導入をする際には、この審査基準及び別票に定める項目に適合することが確認できた場合にのみ実施可能です。また、実施する際には、事前に個人情報保護管理者（個人情報保有課など必要に応じて関連所管課への協議）の決裁後、総括個人情報保護管理者あてに報告が必要です。

オンライン結合・システム導入における別票の確認項目をチェックし、それを添えて、決裁をしてください。

オンライン結合またはシステム導入の内容

（主旨及び開始時期等具体的に記載）

取り扱う個人情報の項目・範囲は必要最小限のものか。

個人情報の項目を具体的に記載

* 新規のシステム構築の場合は、個人情報ファイル簿の作成・公表について区政情報課区政情報係と協議してください。

個人情報ファイルを保有している事業の場合は、ファイル名及びファイル簿番号

- ファイル名：

ファイル簿番号：

取り扱う項目に要配慮個人情報または条例要配慮個人情報が含まれているか。

- 要配慮個人情報 該当無 ・ 該当有
- 条例要配慮個人情報 該当無 ・ 該当有

確認年月日 令和 年 月 日

個人情報保護管理者 部 課長 氏名 _____

担当 係 担当者 連絡先 _____

オンライン結合・システム導入における審査基準（別票） 【根拠：個人情報保護管理基準】（案）

事業検討段階から、以下のすべての各確認項目について確認し「適合」するように検討を進めてください。「適合」しない場合には、事業の見直し等の検討が必要になりますので、あらかじめご承知おきください。「適合」が確認できた場合、各チェック欄に 印をしてください。なお、所管課が事業予定のオンライン結合・システム導入において、確認項目が対象外等の場合は、その旨を具体的に記載してください。

全て確認が終わったら、確認日等を記入するとともに、オンライン結合・システム導入の審査基準に添付してください。

必要に応じて、個人情報の取扱いに関しては区政情報課区政情報係あて、セキュリティ等に関してはDX推進担当課あて、ご相談ください。

No.	確 認 項 目	チェック欄
1	<p>保有個人情報の取扱い</p> <p>1 アクセス制限</p> <p>(1) 個人情報保護管理者は、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を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。</p> <p>() 特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。</p> <p>(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。</p> <p>(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、アクセスは必要最小限としなければならない。</p>	
2	<p>2 複製等の制限</p> <p>職員が業務上の目的で保有個人情報を取り扱う場合であっても、個人情報保護管理者は、次の行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員は、個人情報保護管理者の指示に従い行う。</p> <p>(1) 保有個人情報の複製</p> <p>(2) 保有個人情報の送信</p> <p>(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</p> <p>(4) その他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</p>	
3	<p>3 誤りの訂正等</p> <p>職員は、保有個人情報の内容に誤り等を発見した場合には、個人情報保護管理者の指示に従い、訂正等を行う。</p>	

No.	確認項目	チェック欄
4	<p>4 媒体の管理等</p> <p>職員は、個人情報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施錠できる場所に保管する。取り違えや紛失を防止するため、各媒体の保管場所の区域を定めること。記録されている保有個人情報の性質に応じ、必要があると認めるときは、耐火金庫への保管等を行う。また、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。</p>	
5	<p>5 誤送付等の防止</p> <p>職員は、保有個人情報を含む電磁的記録又は媒体（ ）の誤送信・誤送付、誤交付、又はウェブサイト等への誤掲載を防止するため、個別の事務・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やチェックリストの活用等の必要な措置を講ずる。</p> <p>（ ）文書の内容だけでなく、付加情報（PDFファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。</p>	
6	<p>6 廃棄等</p> <p>職員は、保有個人情報又は保有個人情報が記録されている媒体（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、個人情報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情報の消去又は当該媒体の廃棄を行う。</p> <p>特に、保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合（二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など、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。</p>	
7	<p>7 保有個人情報の取扱状況の記録</p> <p>個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、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。</p>	
8	<p>8 外的環境の把握</p> <p>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じなければならない。</p> <p>（ ）クラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国も該当する。</p>	

No.	確認項目	チェック欄
9	<p>情報システムにおける安全の確保等</p> <p>1 アクセス制御</p> <p>(1) 個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、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()。</p> <p>() アクセス制御の措置内容は、必要最小限のアクセス権限を具体化するものである必要がある。</p> <p>(2) 個人情報保護管理者は、上記(1)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(その定期又は随時の見直しを含む。)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。</p>	
10	<p>2 アクセス記録</p> <p>(1) 個人情報保護管理者は、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、及びアクセス記録を定期的に分析するために必要な措置を講ずる。</p> <p>(2) 個人情報保護管理者は、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。</p>	
11	<p>3 アクセス状況の監視</p> <p>個人情報保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、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表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。</p>	
12	<p>4 管理者権限の設定</p> <p>個人情報保護管理者は、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、当該特権を最小限とする等の必要な措置を講ずる。</p>	
13	<p>5 外部からの不正アクセスの防止</p> <p>個人情報保護管理者は、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。</p>	
14	<p>6 不正プログラムによる漏えい等の防止</p> <p>個人情報保護管理者は、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(導入したソフトウェアを常に最新の状態に保つことを含む。)を講ずる。</p>	

No.	確認項目	チェック欄
15	<p>7 情報システムにおける保有個人情報の処理 職員は、保有個人情報について、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。個人情報保護管理者は、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。</p>	
16	<p>8 暗号化 個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。職員()は、これを踏まえ、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、適切に暗号化を行う。 ()職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。</p>	
17	<p>9 記録機能を有する機器・媒体の接続制限 個人情報保護管理者は、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・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。</p>	
18	<p>10 端末の限定 個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。</p>	
19	<p>11 端末の盗難防止等 (1)個人情報保護管理者は、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、個人情報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서는ならない。</p>	
20	<p>12 第三者の閲覧防止 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。</p>	
21	<p>13 入力情報の照合等 職員は、情報システムで取り扱う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。</p>	
22	<p>14 バックアップ 個人情報保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。</p>	

No.	確認項目	チェック欄
23	<p>1 5 情報システム設計書等の管理</p> <p>個人情報保護管理者は、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、その保管、複製、廃棄等について必要な措置を講ずる。</p>	
24	<p>情報システム室等の安全管理</p> <p>1 入退管理</p> <p>(1) 個人情報保護管理者は、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「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。</p> <p>(2) 個人情報保護管理者は、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の管理の容易化、所在表示の制限等の措置を講ずる。</p> <p>(3) 個人情報保護管理者は、情報システム室等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を設定し、及びパスワード等の管理に関する定めを整備（その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。</p>	
25	<p>2 情報システム室等の管理</p> <p>(1) 個人情報保護管理者は、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、警報装置及び監視設備の設置等の措置を講ずる。</p> <p>(2) 個人情報保護管理者は、災害等に備え、情報システム室等に、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。</p>	
26	<p>情報セキュリティの確保</p> <p>情報セキュリティポリシー等に則ったセキュリティ対策を講じたうえで、取り扱う保有個人情報の性質等に起因するリスクに応じた措置を講じる。</p> <p>(必要に応じて、DX推進担当課に照会及び確認しチェックすること。)</p>	

世田谷区個人情報保護管理基準 (案)

施行日：令和5年4月1日

目次

第1	趣旨	1
第2	個人情報保護管理体制	1
1	総括個人情報保護管理者	1
2	個人情報保護管理者	1
3	個人情報保護担当者	2
4	個人情報保護監査責任者	2
5	個人情報保護管理委員会	2
第3	職員の責務	2
第4	教育研修	2
第5	保有個人情報の取扱い	3
1	アクセス制限	3
2	複製等の制限	3
3	誤りの訂正等	3
4	媒体の管理等	4
5	誤送付等の防止	4
6	廃棄等	4
7	保有個人情報の取扱状況の記録	4
8	外部環境の把握	5
第6	情報システムにおける安全の確保等	5
1	アクセス制御	5
2	アクセス記録	5
3	アクセス状況の監視	5
4	管理者権限の設定	6
5	外部からの不正アクセスの防止	6
6	不正プログラムによる漏えい等の防止	6
7	情報システムにおける保有個人情報の処理	6
8	暗号化	6
9	記録機能を有する機器・媒体の接続制限	6
10	端末の限定	7
11	端末の盗難防止等	7
12	第三者の閲覧防止	7
13	入力情報の照合等	7
14	バックアップ	7
15	情報システム設計書等の管理	7

第7	情報システム室等の安全管理	7
1	入退管理	7
2	情報システム室等の管理	8
第8	保有個人情報の利用及び提供	8
1	保有個人情報の提供における必要な手順	8
2	保有個人情報の提供における特別な措置	8
第9	個人情報の取扱いの委託	9
1	業務の委託等	9
2	その他	11
第10	情報セキュリティの確保	11
第11	安全管理上の問題への対応	11
1	事案の報告及び再発防止措置	11
2	法に基づく報告及び通知	12
3	公表等	12
第12	監査及び点検の実施	12
1	監査	12
2	点検	12
3	評価及び見直し	13
別紙1	個人情報を取り扱う業務の外部委託基準	14
別紙2	個人情報を取り扱う業務委託の特記事項	15
参考1	電算処理の外部委託基準	17
参考2	電算処理の業務委託契約の特記事項 (兼電算処理の個人情報を取り扱う業務委託契約の特記事項)	19

第1 趣旨

この基準は、令和5年4月1日に施行される改正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66条第1項の規定等及び改正世田谷区個人情報保護条例（令和5年3月条例第〇号。以下「条例」という。）第3条第2項の規定等を踏まえ、各実施機関が保有する個人情報の安全管理のために必要かつ適切な措置として基準を定めるものである。

各実施機関においては、この基準に則り、保有個人情報の漏えい等が生じた場合に区民が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報を記録した媒体の性質等に起因するリスクに応じて、個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

また、電子計算機を用いて保有個人情報を取り扱う場合においては、世田谷区電子計算組織の運営に関する規則（平成16年4月世田谷区規則第47号）第5章に規定する情報セキュリティポリシー及び学校教育に供する電子計算組織の運営に関する規則（平成20年3月世田谷区教育委員会規則第9号）第6章に規定する情報セキュリティ対策（以下「情報セキュリティポリシー等」という。）に則ったセキュリティ対策を講じたうえで、取り扱う保有個人情報の性質等に起因するリスクに応じた措置を講じなければならない。

なお、国が示す「行政機関等の保有する個人情報の適切な管理のための措置に関する指針」が改定された場合のほか必要に応じて、この基準を見直すものとする。

第2 個人情報保護管理体制

1 総括個人情報保護管理者

世田谷区副区長の担当事項に関する規程に基づき総務部を担任する副区長を総括個人情報保護管理者とする。総括個人情報保護管理者は、各実施機関における保有個人情報の管理に関する事務を総括する任に当たる。

2 個人情報保護管理者

保有個人情報を取り扱う各課に個人情報保護管理者を一人置き、課長をもって充てる。個人情報保護管理者は、各課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。保有個人情報を情報システムで取り扱う場合、個人情報保護管理者は、情報化管理者として、本基準のほか、情報セキュリティポリシー等に則った措置が講じられていることを確認する。

3 個人情報保護担当者

保有個人情報を取り扱う各課に、当該課の個人情報保護管理者が指定する個人情報保護担当者を置く。個人情報保護担当者は、個人情報保護管理者を補佐し、各課における保有個人情報の管理に関する事務を担当する。

4 個人情報保護監査責任者

総務部長をもって充てる。個人情報保護監査責任者は、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。

5 個人情報保護管理委員会

総括個人情報保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため個人情報保護管理委員会を設け、定期に又は随時に開催する。この委員会は、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。

第3 職員の責務

職員は、法及び条例の趣旨に則り、関連する法令及び規程等の定め並びに総括個人情報保護管理者、個人情報保護管理者及び個人情報保護担当者の指示に従い、保有個人情報を適切に取り扱わなければならない。

第4 教育研修

- 1 総括個人情報保護管理者は、保有個人情報の取扱いに従事する職員(派遣労働者を含む。以下同じ。)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 総括個人情報保護管理者は、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報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 総括個人情報保護管理者は、個人情報保護管理者及び個人情報保護担当者に対し、課の保有個人情報の適切な管理のための教育研修を定期的実施する。

- 4 個人情報保護管理者は、当該課の職員に対し、保有個人情報の適切な管理のために、総括個人情報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5 保有個人情報の取扱い

1 アクセス制限

- (1) 個人情報保護管理者は、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を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。
- () 特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。
- (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、アクセスは必要最小限としなければならない。

2 複製等の制限

職員が業務上の目的で保有個人情報を取り扱う場合であっても、個人情報保護管理者は、次の行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員は、個人情報保護管理者の指示に従い行う。

- (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) その他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

3 誤りの訂正等

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

4 媒体の管理等

職員は、個人情報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施錠できる場所に保管する。取り違えや紛失を防止するため、各媒体の保管場所の区域を定めること。記録されている保有個人情報の性質に応じ、必要があると認めるときは、耐火金庫への保管等を行う。また、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。

5 誤送付等の防止

職員は、保有個人情報を含む電磁的記録又は媒体（ ）の誤送信・誤送付、誤交付、又はウェブサイト等への誤掲載を防止するため、個別の事務・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やチェックリストの活用等の必要な措置を講ずる。

（ ）文書の内容だけでなく、付加情報（PDFファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。

6 廃棄等

職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバーに内蔵されているものを含む。）が不要となった場合には、個人情報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情報の消去又は当該媒体の廃棄を行う。

特に、保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合（二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など、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。

7 保有個人情報の取扱状況の記録

個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、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。

8 外的環境の把握

保有個人情報、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じなければならない。

()クラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国も該当する。

第6 情報システムにおける安全の確保等

1 アクセス制御

(1) 個人情報保護管理者は、保有個人情報(情報システムで取り扱うものに限る。以下第6(情報システムにおける安全の確保等)(13を除く。)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()。

()アクセス制御の措置内容は、第5(保有個人情報の取扱い)1(1)により設定した必要最小限のアクセス権限を具体化するものである必要がある。

(2) 個人情報保護管理者は、上記(1)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(その定期又は随時の見直しを含む。)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。

2 アクセス記録

(1) 個人情報保護管理者は、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、及びアクセス記録を定期的に分析するために必要な措置を講ずる。

(2) 個人情報保護管理者は、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。

3 アクセス状況の監視

個人情報保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、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表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。

4 管理者権限の設定

個人情報保護管理者は、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、当該特権を最小限とする等の必要な措置を講ずる。

5 外部からの不正アクセスの防止

個人情報保護管理者は、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。

6 不正プログラムによる漏えい等の防止

個人情報保護管理者は、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(導入したソフトウェアを常に最新の状態に保つことを含む。)を講ずる。

7 情報システムにおける保有個人情報の処理

職員は、保有個人情報について、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。個人情報保護管理者は、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。

8 暗号化

個人情報保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。職員()は、これを踏まえ、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、適切に暗号化を行う。

()職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。

9 記録機能を有する機器・媒体の接続制限

個人情報保護管理者は、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・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。

1 0 端末の限定

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

1 1 端末の盗難防止等

- (1) 個人情報保護管理者は、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、個人情報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서는ならない。

1 2 第三者の閲覧防止

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ないよう、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。

1 3 入力情報の照合等

職員は、情報システムで取り扱う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。

1 4 バックアップ

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

1 5 情報システム設計書等の管理

個人情報保護管理者は、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 情報システム室等の安全管理

1 入退管理

- (1) 個人情報保護管理者は、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「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) 個人情報保護管理者は、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の管理の容易化、所在表示の制限等の措置を講ずる。
- (3) 個人情報保護管理者は、情報システム室等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を設定し、及びパスワード等の管理に関する定めを整備（その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。

2 情報システム室等の管理

- (1) 個人情報保護管理者は、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、警報装置及び監視設備の設置等の措置を講ずる。
- (2) 個人情報保護管理者は、災害等に備え、情報システム室等に、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8 保有個人情報の利用及び提供

1 保有個人情報の提供における必要な手順

個人情報とは、法令の定める所掌事務を遂行するために必要な場合に限り保有するものであり、利用目的はできる限り特定しなければならず、その利用目的を超えて保有個人情報を利用又は提供することは原則として禁止されている。

法第69条に定められている場合のみ利用又は提供が可能となるため、利用又は提供を求められた場合、同条に照らし合わせてその可否を適切に検討しなければならない。

各課の個人情報保護管理者は、利用又は提供を行うにあたり、情報公開・個人情報保護審議会の意見を踏まえ、区として作成した「審査基準」を用いてその可否を判断する。個人情報保護管理者は、各「審査基準」を取りまとめ、総括個人情報保護管理者あてに提出する。

なお、同条は、利用又は提供についての制限に関する規定であり、仮に、同条の規定で利用又は提供が可能となる場合であっても、安易な利用又は提供を行わないよう、注意しなければならない。

2 保有個人情報の提供における特別な措置

- (1) 個人情報保護管理者は、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、上記のとおり、「審査基準」に基づき可否を判断するほか、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。)を取り交わすことが必要である。

- () 法第 69 条第 2 項第 3 号について、国の行政機関を除く機関の一部(例：独立行政法人国立病院機構)においては、法第 5 章第 2 節ではなく第 4 章(個人情報取扱事業者等の義務等)が適用される。そのため、区(行政機関等)と同等の安全管理措置が取られているとは言えないことから、個人情報が適切に取り扱える体制であることを確認する必要がある。
- (2) 個人情報保護管理者は、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) 個人情報保護管理者は、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、上記(1)及び(2)に規定する措置を講ずる。

第 9 個人情報取扱いの委託

1 業務の委託等

- (1) 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、「個人情報を取り扱う業務の外部委託基準」(別紙 1)に則り、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。なお、委託する業務に電算処理に係る業務が含まれる場合においては、「電算処理の外部委託基準」(参考 1)に則り、必要な措置を講ずる。

また、契約に際しては、次に記載する から までの事項を明記した「個人情報を取り扱う業務委託の特記事項」(別紙 2)(又は「電算処理の業務委託契約の特記事項(兼電算処理の個人情報を取り扱う業務委託契約の特記事項)」(参考 2))に記載されている内容を相手方に遵守させなければならない。

各課の個人情報保護管理者は、外部委託を行うにあたっては、第 8(保有個人情報の利用及び提供)の方法と同様に、情報公開・個人情報保護審議会の意見を踏まえ、区として作成した「審査基準」を用いてその可否を判断した後、各「審査基準」を取りまとめ、総括個人情報保護管理者あてに提出する。

なお、()のとおり、「契約書」を取り交わさない又は支出が伴わない場合等においても、外部の者に個人情報を取り扱わせる場合は、法第66条における安全管理措置の対象となる場合がある。この場合、当該業務においては外部委託基準を遵守する必要があることに留意する。

加えて、委託先に対して必要かつ適切な監督を行っていない場合で、委託先(再委託先を含む。)が個人情報について不適切な取扱いを行ったときは、委託元である区による法違反と判断され得ることから、委託先における個人情報の取扱い状況を必要に応じ又は随時に確認できるよう体制を整える必要がある。

()「委託」とは、契約の形態・種類を問わず、実施機関が他の者に個人情報の取扱いを行わせることをいう。具体的には、個人情報の入力(本人からの取得を含む。)、編集、分析、出力等の処理を行うことを委託すること等が想定されるが、これらに限られない。

個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務に関する事項

個人情報の複製等の制限に関する事項

再委託(再委託先が委託先の子会社(会社法(平成17年法律第86号)第2条第1項第3号に規定する子会社をいう。)である場合も含む。)の原則禁止に関する事項

個人情報の安全管理措置に関する事項

個人情報の漏えい等の事案の発生時における対応に関する事項

委託終了時における個人情報の消去及び媒体の返却に関する事項

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

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い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やその量等に応じて、作業の管理体制及び実施体制や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、委託先に上記(1)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

元自らが上記(3)の措置を実施する。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個人情報の取扱いに関する事項を明記する。

2 その他

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などを考慮し、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10 情報セキュリティの確保

情報セキュリティポリシー等に則ったセキュリティ対策を講じたうえで、取り扱う保有個人情報の性質等に起因するリスクに応じた措置を講じる。

第11 安全管理上の問題への対応

1 事案の報告及び再発防止措置

- (1) 保有個人情報の漏えい等安全管理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場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する個人情報保護管理者に報告する()。

()職員は、当該事案の発生(事案発生のおそれを含む。)を認識した場合、時間を要する事実確認を行う前に、個人情報保護管理者に報告する。

- (2) 個人情報保護管理者は、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や不正プログラムの感染が疑われる当該端末等のLANケーブルを抜くなど、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) 個人情報保護管理者は、事案の発生した経緯、被害状況等を調査し、総括個人情報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、直ちに総括個人情報保護管理者に当該事案の内容等について報告する。

- (4) 総括個人情報保護管理者は、上記(3)による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、被害状況等を区長に速やかに報告する。
- (5) 個人情報保護管理者は、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部署に再発防止措置を共有する。

2 法に基づく報告及び通知

法第68条第1項の規定による、次に記載の(1)から(5)までのいずれかに該当する漏えい等の事態において、国の個人情報保護委員会(以下「委員会」という。)への報告及び同条第2項の規定による本人への通知を要する場合には、上記1(1)から(5)までの対応と並行して、速やかに委員会への報告等所定の手続を行うとともに、委員会による事案の把握等に協力する。

- (1) 要配慮個人情報が含まれる保有個人情報(高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下(2)から(5)までにおいて同じ。)の漏えい等が発生し、又は発生したおそれがある事態
- (2) 不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態
- (3) 不正の目的をもって行われたおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態
- (4) 保有個人情報に係る本人の数が100人を超える漏えい等が発生し、又は発生したおそれがある事態
- (5) 条例要配慮個人情報が含まれる保有個人情報の漏えい等が発生し、又は発生したおそれがある事態

3 公表等

法第68条第1項の規定による委員会への報告及び同条第2項の規定による本人への通知を要しない場合であっても、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、当該事案に係る保有個人情報の本人への連絡等の措置を講ずる。

区民の不安を招きかねない事案(例えば、公表を行う漏えい等が発生したとき、個人情報保護に係る内部規程に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等)については、当該事案の内容、経緯、被害状況等について、委員会へ情報提供を検討し速やかに必要な対応をとる。

第 1 2 監査及び点検の実施

1 監査

個人情報保護監査責任者は、保有個人情報の適切な管理を検証するため、上記の第 2（個人情報保護管理体制）から第 1 1（安全管理上の問題への対応）までに記載する措置の状況を含む当該実施機関における保有個人情報の管理の状況について、定期的に、及び必要に応じ随時に監査（外部監査を含む。以下同じ。）（ ）を行い、その結果を総括個人情報保護管理者に報告する。

（ ）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。

2 点検

個人情報保護管理者は、各課における保有個人情報の記録媒体、処理経路、保管方法等について、定期的に、及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括個人情報保護管理者に報告する。

3 評価及び見直し

総括個人情報保護管理者、個人情報保護管理者等は、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。

別紙 1 (第 9 関係)

個人情報を取り扱う業務の外部委託基準

1 外部委託における基本的な考え方

- (1) 委託する個人情報の項目を特定し、必要最小限度の範囲で取り扱わせることができる状態で委託を行う。必要に応じて仮名・匿名化も検討すること。
- (2) 委託先(再委託先を含む。以下同じ。)が本基準における「外部委託における条件」を遵守できる者であることを確認しなければならない。
- (3) 委託する業務に電算処理に係る業務が含まれる場合においては、「電算処理の外部委託基準」を満たしていなければならない。

2 外部委託における条件

個人情報を取り扱う業務を外部委託する場合には、次に掲げる事項を当該委託の条件としなければならない。各条件の具体的内容については、「個人情報を取り扱う業務委託契約の特記事項」に示す。

なお、特記事項を付さない(契約を締結しない)委託を行う場合においても、必ず同条件を付さなければならないことに留意すること。

- ・ 秘密保持義務
- ・ 目的外使用及び外部提供の禁止
- ・ 複写等の禁止
- ・ 再委託の禁止
- ・ 安全管理体制等の通知
- ・ 委託終了時における個人情報の消去及び媒体の返却
- ・ 漏えい等の対応
- ・ 監査、施設への立入検査の受入れ
- ・ 契約解除及び損害賠償責任の定め

(案)

別紙 2 (第 9 関係)

個人情報を取り扱う業務委託の特記事項

(秘密保持義務)

1 受託者は、この契約の履行により直接又は間接に知り得た個人情報を、第三者に漏らしてはならない。また、契約期間満了後も同様とする。

(書面主義の原則)

2 受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。

(管理体制等の通知)

3 受託者は、この契約の締結後直ちに、以下の文書を委託者に提出しなければならない。

(1) 個人情報保護に関する社内規程又は基準

(2) 以下の内容を含む従事者名簿

個人情報を取り扱う者の氏名、責任及び役割

委託業務において個人情報の授受に携わる者の氏名及び業務執行場所

緊急連絡先一覧

(3) 委託業務に係る実施スケジュールを明記した文書

(再委託の禁止)

4 受託者は、この契約による業務を第三者に再委託してはならない。ただし、当該業務の全部又は一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容を委託者に通知し、委託者の承諾を得なければならない。また、再受託者(委託先の子会社(会社法(平成17年法律第86号)第2条第1項第3号に規定する子会社をいう。)である場合も含む。)にも、この契約を遵守させなければならない。

(目的外使用及び外部提供の禁止)

5 受託者は、個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。

(複写及び複製の禁止)

6 受託者は、個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。

- 7 委託者の許可を受けて複写又は複製したときは、委託業務の終了後直ちに当該複写物又は複製物を利用できないよう処分又は委託者へ提出しなければならない。

(安全管理措置の実施)

- 8 受託者は、委託業務において、委託者に提出した個人情報保護に関する社内規程又は基準を遵守しなければならない。
- 9 受託者は、従事者に対して、個人情報に関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。
- 10 受託者は、個人情報の授受、保管及び管理について、善良な管理者の注意をもって当たり、個人情報の漏えい、滅失、毀損等(以下「漏えい等」という。)の事故を防止しなければならない。

(委託終了時における個人情報の消去及び媒体の返却)

- 11 受託者は、委託業務が終了したときは、直ちに、委託業務に使用した個人情報の消去及び個人情報記録された媒体の返却をしなければならない。

(委託業務の報告)

- 12 受託者は、委託者に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。

(監査、施設への立入検査の受入れ)

- 13 受託者は、委託者が必要とする場合、監査又は検査を受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。
- 14 受託者は、委託者が必要とする場合は、業務執行場所へ委託者の職員の立入りを認めるものとする。

(個人情報の漏えい等の対応)

- 15 受託者は、個人情報の漏えい等が生じたとき、又は漏えい等が生じたおそれがあるときには直ちに委託者に対して連絡するとともに、遅滞なくその状況について書面をもって委託者に報告し、委託者の指示に従わなければならない。

(契約解除及び損害賠償)

- 16 受託者が、個人情報の取扱いについて法令及び本特記事項に違反した場合、委託者は契約解除を申し出ることができる。また、受託者が、個人情報の取扱いにつき法令及び本特記事項に違反したことにより、委託者に損害が生じた場合には、これを賠償するものとする。

参考 1

【現行】 電算処理の外部委託基準

第 1 目的

電算処理に係わる業務を外部委託する場合において、世田谷区の定める情報セキュリティ水準を確保するため、世田谷区情報セキュリティ対策基準に基づき、委託先による業務の遂行を契約等により適切に管理する必要がある。本基準は、委託元である世田谷区の職員が、委託先を適切に管理する上で、遵守すべき事項について定めることを目的とする。

第 2 対象者

本基準の対象者は、情報システム及び電算処理業務を外部委託し、委託元として業務を行う全ての職員及び情報セキュリティ管理者を対象とする。

第 3 外部委託先の管理

電算処理を外部委託する場合においては、次に掲げる事項を確認しなければならない。

- 1 電算処理の外部委託により、情報資産及び個人情報の保護に支障が生ずることがないこと。
- 2 電算処理の外部委託の契約相手方が、本基準の「第 4 外部委託契約における条件」を遵守できる管理体制及び設備を有する者であること。
- 3 外部委託先の選定にあたり「第 4 外部委託契約における条件」に基づき、委託内容に応じた情報セキュリティ対策が確保されること。

第 4 外部委託契約における条件

電算処理を外部委託する場合においては、次に掲げる事項を当該契約の条件としなければならない。なお、各契約条件の具体的内容については、別紙「電算処理の業務委託契約の特記事項（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）」に示す。

- ・ 秘密保持義務
- ・ 管理体制等の通知
- ・ 再委託の禁止
- ・ 目的外利用の禁止
- ・ 業務執行場所、業務日程の通知
- ・ 物理的セキュリティ対策

- ・ 人的セキュリティ対策
- ・ 技術的及び運用におけるセキュリティ対策
- ・ データのセキュリティ対策
- ・ 電算処理機器の修理又は廃棄
- ・ 委託業務の報告
- ・ 監査、施設への立入り検査の受入れ
- ・ 緊急時の対応
- ・ サービスレベルの保証
- ・ 損害賠償

第5 確認・措置等

外部委託に関する管理責任を有する委託元部門責任者及び担当者は、外部委託事業者において必要なセキュリティ対策が、外部委託契約における条件に基づき確保されていることを定期的に確認し、その内容をネットワーク管理者に報告するとともに、その重要度に応じその重要度に応じて統括情報セキュリティ責任者に報告しなければならない。

参考 2

【案】

電算処理の業務委託契約の特記事項 (兼電算処理の個人情報を取り扱う業務委託契約の特記事項)

(秘密保持義務)

- 1 受託者は、当該委託契約（業務内容に保守委託を伴う賃貸借契約等を含む。以下同じ。）に係る電算処理業務（以下「委託業務」という。）により知り得た個人情報その他の情報（以下「情報」という。）を、いかなる理由があっても第三者に漏らしてはならず、この旨を委託業務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。また、契約期間満了後も、同様とする。

(書面主義の原則)

- 2 受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。

(管理体制等の通知)

- 3 受託者は、当該委託契約の締結後直ちに、以下の文書を区に提出しなければならない。提出後に内容の変更があった場合も、同様とする。
 - (1) 情報セキュリティ及び個人情報保護に関する社内規程又は基準
 - (2) 以下の内容を含む従事者名簿
電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所
委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所
委託業務に関する緊急時連絡先一覧
 - (3) 委託業務に係る実施スケジュールを明記した文書
 - (4) 委託業務において使用する情報システムのネットワーク構成図（特定個人情報ファイル（コンピュータ等で検索することができるよう体系的に構成した情報の集合体であって、個人番号をその内容に含むもの。以下同じ。）を取り扱う場合のみ。第 23 項の事項を証するもの。）
 - (5) 委託業務において使用する情報システムのセキュリティ仕様書（特定個人情報ファイルを取り扱う場合のみ。第 24 項の事項を証するもの。）
 - (6) クラウドサービス（有料、無料に関わらず、民間事業者等がインターネット上で提供する情報処理サービスで、約款への同意及び簡易なアカウントの登録等により当該機能が利用可能となるサービスのこと。以下同じ。）利用に係るリスク対策文書（委託業務においてクラウドサービスを利用する場合のみ。第 25 項の事項を証するもの。）

(再委託の禁止)

- 4 受託者は、委託業務の全部又は一部を、他の者に再委託してはならない。ただし、附属業務でやむを得ず再委託する必要があるときは、受託者は、再受託者（委託先の子会社（会社法（平成17年法律第86号）第2条第1項第3号に規定する子会社をいう。）である場合も含む。以下同じ。）に当該委託契約及び本特記事項を遵守させ、かつ、再受託者にかかる再委託の内容及び第3項に規定する事項を、区に事前に書面をもって通知し、その承認を得なければならない。
- 再受託者も、委託業務の全部又は一部を、他の者に更に再委託してはならない。附属業務でやむを得ず更に再委託する必要があるときは、再委託と同様の条件と手続きにより、区の承認を得なければならない。更に再委託が繰り返される場合も同様とする。

(目的外使用等及び複写等の禁止)

- 5 受託者は、委託業務で取り扱う情報を委託業務の目的以外に使用してはならない。また、第三者に提供してはならない。
- 6 受託者は、区が委託業務での使用を目的として受託者に提供し、又は貸与する情報及び情報資産（世田谷区電子計算組織の運営に関する規則（平成16年世田谷区規則第47号）第2条第9号に規定する情報資産をいう。以下同じ。）を、委託業務以外の目的に使用してはならない。
- 7 受託者は、委託業務で取り扱う情報及び情報資産について、業務上必要なバックアップを取得する場合を除き、区の承認を得ずに複写してはならない。委託業務を実施する上でやむを得ず複写するときは、あらかじめ区に通知し、その承認を得なければならない。この場合において、委託業務の終了後、受託者は、直ちに複写した情報及び情報資産を消去又は廃棄し、使用できない状態にするとともに、情報及び情報資産を消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。
- 8 受託者は、区の事前の承諾なく、委託業務で取り扱う情報及び情報資産を区の事業所または受託者の事業所から持ち出してはならない。

(物的セキュリティ対策)

- 9 受託者は、委託業務に使用する情報システムに係る装置の取付けを行う場合は、できる限り、火災、水害、埃、振動、温度、湿度等の影響を受けない場所に設置するものとし、施錠等容易に取り外すことができないよう必要な措置を講じなければならない。
- 10 受託者は、委託業務に係る区が運用する情報システムのサーバ等を区庁舎外に設置する場合は、区の承認を得なければならない。また、定期的に当該サーバ等への情報セキュリティ対策状況について確認するとともに、区から要請があった場合は、その結果を区に報告しなければならない。

- 11 受託者は、その従事者に名札等の着用及び身分証明書等の携帯を義務付け、区の情報システム室その他の区の管理区域に立ち入る場合において区から求められたときは、身分証明書等を提示するよう指導しなければならない。
- 12 受託者は、委託業務で使用するパソコン等の盗難を防止するため、当該パソコン等をセキュリティワイヤーで固定し、又は従事者が業務執行場所を離れる間において施錠可能なロッカー等に収納させるなどの措置を講じなければならない。

(人的セキュリティ対策)

- 13 受託者は、委託業務において、区に提出した情報セキュリティ及び個人情報保護に関する社内規程又は基準を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに区に報告し、代替策について協議しなければならない。
- 14 受託者は、情報及び情報資産を適切に保管するものとし、パソコン等により情報及び情報資産を使用する場合は、第三者に使用され、又は閲覧されることがないように、離席時にパスワードロック又はログオフ等を行わなければならない。
- 15 受託者は、従事者に情報システムの保守又は運用業務に関し、次の事項を遵守させなければならない。
 - (1) 自己が利用している ID は、他人に利用させないこと (ID の共用を指定されている場合は除く。)。
 - (2) 共用 ID を利用する場合は、共用 ID の利用者以外の者に利用させないこと。
 - (3) パスワードを秘密にし、パスワードの照会等には一切応じないこと (パスワード発行業務を除く。)。
 - (4) パスワードのメモの不用意な作成等により、パスワード流出の機会を作らないこと。
 - (5) パスワードは、十分な長さとし、想像し難い文字列とすること。
 - (6) 複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しないこと。
 - (7) パソコン等のパスワードの記憶機能を利用しないこと。
 - (8) 社員間でパスワードを共有しないこと (ID の共用を指定されている場合を除く。)。
- 16 受託者は、従事者に対して、情報セキュリティに関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。

(技術的及び運用におけるセキュリティ対策)

- 17 受託者は、情報システムの保守又は運用業務を遂行するに当たり、情報システムの変更記録、作業日時及び実施者を記録するとともに、各種アクセス

記録及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。

- 18 受託者は、アクセスログ等を取得するサーバについて、正確な時刻設定を行わなければならない。自動的にサーバ間の時刻同期が可能な場合は、その措置を講じなければならない。
- 19 受託者は、情報システム等に記録された重要性の高い情報について、定期的にバックアップを取得しなければならない。また、バックアップの取得前にその手法を区に通知し、承認を得なければならない。
- 20 受託者は、情報システムの開発及び導入に当たり、開発及び導入前に区と協議の上、情報セキュリティに係る検証事項を定め、検証を実施しなければならない。
- 21 受託者は、委託業務に使用する情報システムがネットワークに接続されている場合は、不正アクセスを防ぐため、常にセキュリティホールの発見に努め、メーカー等からのセキュリティ修正プログラムの提供があり次第、情報システムへの影響を確認し、区と協議の上、修正プログラムを適用しなければならない。また、ウィルスチェックを行い、ウィルスの情報システムへの侵入及び拡散を防止しなければならない。
- 22 受託者は、情報システムを開発する場合は、システム開発及びテスト環境と、本番運用環境を分離しなければならない。
- 23 受託者は、委託業務において特定個人情報ファイルを取り扱う場合は、当該特定個人情報ファイルをインターネットから物理的又は論理的に分離された環境にて取り扱わなければならない。
- 24 受託者は、委託業務に使用する情報システムにおいて特定個人情報ファイルを取り扱う場合は、定期に及び必要に応じ随時に当該情報システムのログ等の分析を行うなど不正アクセス等を検知する仕組みを講じるとともに、当該情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講じなければならない。
- 25 受託者は、委託業務においてクラウドサービスを利用する場合は、当該クラウドサービスの利用に伴い想定される情報セキュリティ上のリスクを回避するために必要な措置を講じなければならない。（例：当該クラウドサービス提供事業者が公表している情報セキュリティ対策内容の確認、受託者が従業員に付与するクラウドサービス用 ID の適切な付与管理、クラウドサービス上に記録した情報が第三者に提供される場合についての確認、サービス利用終了時のデータの取扱い条件の確認、等）

（データのセキュリティ対策）

- 26 受託者は、委託業務に関し、区より情報及び情報資産を受領した場合は、預かり証を区に対して交付しなければならない。また、当該情報及び情報資産を適切に管理するため、情報及び情報資産の受領日時、受領者名、受領し

た情報及び情報資産の種類等の記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を区に提示しなければならない。

- 27 受託者は、委託業務に係る重要度の高い情報及び情報資産を運搬する場合は、可能な限り暗号化、パスワード設定等の保護対策を行い、鍵付きのケース等に格納する等、情報及び情報資産の滅失や不正利用を防止するための処置を講じなければならない。また、重要度の高い情報を電子メール等で送受信する場合は、暗号化、パスワード設定等の保護対策を行わなければならない。
- 28 受託者は、委託業務で取り扱う情報及び情報資産を施錠可能な金庫、ロッカー等に適切に保管する等善良な管理者の注意をもって当たり、情報及び情報資産の取扱いには十分注意し、情報及び情報資産の滅失、毀損及び漏えい等の防止に努めなければならない。
- 29 受託者は、委託業務が終了したときは、区より受領した情報及び情報資産を速やかに区に返却しなければならない。また、返却が不可能な情報及び情報資産は、区の了承のもと、バックアップデータを含め、情報及び情報資産を使用できないように処置した上で消去又は廃棄し、日時、担当者及び処理内容を区に報告しなければならない。
- 30 受託者は、情報資産の作成業務を終了したときは、直ちに当該情報資産を区があらかじめ指定した職員に引き渡さなければならない。

(電算処理機器の廃棄)

- 31 受託者は、委託業務で使用しているサーバ、パソコン等の機器(以下これらを「電算処理機器」という。)を廃棄する場合は、事前に当該電算処理機器に保存されている情報及び情報資産を消去、復元できない状態にした上で廃棄しなければならない。

(委託業務の報告)

- 32 受託者は、区に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。

(監査、施設への立入検査の受入れ)

- 33 受託者は、情報及び情報資産の情報セキュリティ管理状況について、区の求めに応じて報告するものとする。また、区が必要に応じて監査又は検査を実施する場合は受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。
- 34 受託者は、区が必要とする場合は、業務執行場所へ区の職員の立入りを認めるものとする。

(緊急時の対応)

35 受託者は、委託業務において、業務上のトラブル、災害、事故、電算処理機器の不良、故障及び破損等が発生した場合は、直ちに区にその状況について報告し、区の指示に従わなければならない。

36 受託者は、委託業務について次に掲げる事象が発生した又は発生したおそれがある場合は、遅滞なく、区にその状況を具体的に報告しなければならない。

- (1) 情報及び情報資産の滅失
- (2) 情報及び情報資産の毀損
- (3) 情報の漏えい
- (4) 不正アクセス
- (5) 情報セキュリティポリシーの違反
- (6) 前各号に掲げるもののほか、情報セキュリティに悪影響を及ぼす事象

(サービスレベルの保証)

37 受託者は、委託業務のサービスレベルについて、事前に区と合意している場合は、そのサービスレベルを保証するものとする。

(契約解除及び損害賠償)

38 受託者が、本特記事項に違反した場合、区は契約解除を申し出ることができ。また、受託者は、本特記事項に違反し、又は本特記事項を履行しなかったことにより、区に損害が生じた場合には、区に対しこれを賠償するものとする。

諮問第994号「個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱いに関する運用上の細則等について」に係る質問及び回答

令和4年12月13日

No.	質 問	回 答
1	<p>資料2 - 1・法改正に基づく区の対応について 所管課が適切にチェックの言葉が羅列されていますが、適切の言葉は、逃げ道があるように感じました。この文言の確定した経緯を教えてください。例 厳密 など</p>	<p>法第66条第1項において、区を含む行政機関等は「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じなければならない」とされており。 ご質問の「法改正に基づく区の対応」については、安全管理のために必要な措置として各「審査基準」を策定し、これを適切にチェックすることで法の要求を満たすことができる、という趣旨で「適切」という文言を用いています。</p>
2	<p>資料1 2 個人情報保護管理基準のところ、各自治体は、当該ガイドに則り、安全管理措置を講ずべく個人情報保護管理基準を策定することとなったとありますが、現在ある審議会が今後どのように関わっていくのか、関わり方がよく分からない。</p>	<p>世田谷区個人情報保護管理基準は、法第66条第1項に規定される安全管理措置の一環として区内部の個人情報の管理について新たに定めるものとなります。特に、外部委託等の審査基準は、令和4年7月の審議会答申第968号でご意見をいただきました「内部管理としての庁内のチェック体制」を構築するために策定するものです。 この個人情報保護管理基準に審議会の意見を取り入れ、必要に応じて内容を見直すことにより、従来から審議会が担ってきた住民監視の役割を今後も果たしていただくこととなります。</p>
3	<p>資料2 ・個人情報を保有する際に個人情報ファイル簿、条例個人情報ファイル簿を作成することには異存はありませんが、審査基準や審査基準（別票）をたとえ1件の個人情報を区が取得、保有する際にも提出しなければいけないということなのでしょうか？ 例えば、地域の方に呼び掛けてお集まりいただいた会議でお名前を頂くような場合でもこのような手続きを取らないといけないのですか？</p>	<p>個人情報ファイル簿及び条例個人情報ファイル簿については、保有個人情報を含む情報の集合体である個人情報ファイルを保有する際に作成・公表するものであり、複数の個人情報を保有し、かつ、当該個人情報を利用し体系的に構築した場合となります。 そのため、ご質問のような場合は、個人情報ファイル簿の作成は必要ありませんが、ご指摘のとおり、各所管課は、総括個人情報保</p>

もしそうだとするならば、この手続きは1,000人以上の場合、要配慮個人情報、条例要配慮個人情報などを保有する際に限って行うようにした方がいいのではないのでしょうか。これでは事務が煩雑になりすぎてしまうのではないかと思いました。

管理者に審査基準及び審査基準（別票）の提出が必要になることが想定されます。

しかしながら、ご指摘、ご心配いただいているとおり、各所管課の事務が非常に煩雑になることが想定されます。こうしたことから、各所管課は、要配慮個人情報や条例要配慮個人情報を保有する場合等に限定して、総括個人情報保護管理者に審査基準及び審査基準（別票）を提出させる仕組みとすることを検討してまいります。

(案)

個人情報の保護に関する法律の改正に伴う世田谷区の
個人情報の取扱いに関する運用上の細則等について

答 申

(令和4年12月)

世田谷区情報公開・個人情報保護審議会

はじめに

今般の個人情報保護法の改正について、審議会は、世田谷区長からの令和4年2月10日付諮問第968号「令和3年個人情報保護法改正に伴う世田谷区における個人情報保護制度等の見直しに向けての考え方について」に対し、令和4年7月に答申しました。その後、世田谷区において、世田谷区個人情報保護条例の全部改正(素案)を取りまとめ、9月からはパブリックコメント(区民意見提出手続)を実施するなど、個人情報保護制度等の見直しに継続して取り組んできたことと承知しています。

こうした中、世田谷区長より審議会に対し、同年10月18日付諮問第994号「個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱いに関する運用上の細則等について」が諮問されました。これに対し、審議会では、審議会小委員会を設置し2回にわたり検討、審議を行い、同年11月30日に小委員会から審議会に検討結果が報告されたところです。

これを踏まえ、改めて、審議会において諮問の内容を審議し、各委員からの意見や質問等を検討し整理した結果を本答申として取りまとめました。

本年7月の答申の折にも記していますが、重要なことですので、再度、確認として記します。

審議会としては、この法改正の趣旨を踏まえたうえで、国の制度に先駆け世田谷区が個人情報保護制度を構築し、一貫して区民の個人情報保護のために多くのことを積み上げてきた知見と実績を大切に、今後も継続・発展させていくことが、必要不可欠であると考えています。

これから世田谷区が条例改正案の策定及び事務運用の検討を行ううえでも、本答申をもとに世田谷区個人情報保護条例が改正され、それに基づく新たな個人情報保護制度が運用されることにより、世田谷区の個人情報保護制度がより充実したものとなることを期待します。

令和4年12月15日

世田谷区情報公開・個人情報保護審議会

会 長 山 田 健 太

目 次

1	条例要配慮個人情報の制定	1
2	個人情報保護管理基準	2
3	外部委託等の審査基準	3
4	開示請求手続の本人確認書類	4
5	死者の情報に関する開示請求基準	4
参考 1	諮問文（令和 4 年 1 0 月 1 8 日付） 「個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の 取扱いに関する運用上の細則等について」	6
参考 2	世田谷区情報公開・個人情報保護審議会委員名簿	7
参考 3	小委員会の審議経過	8

1 条例要配慮個人情報の制定

(1) 改正個人情報の保護に関する法律第60条第5項(条例要配慮個人情報)について

改正個人情報の保護に関する法律(以下「改正法」という。)では、第2条第3項で「要配慮個人情報」(人種、信条、社会的身分等)を定めている。また、第60条第5項で「地域の特性その他の事情に応じて、本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして地方公共団体が条例で定める記述等が含まれる個人情報」(いわゆる「条例要配慮個人情報」)を定め、「要配慮個人情報」に該当しない「条例要配慮個人情報」を条例で定めることができる旨規定している。

一方、現行の世田谷区個人情報保護条例(以下「条例」という。)では、第7条で「収集禁止事項」を定め、原則として、思想、信条及び宗教に関する事項、社会的差別の原因となる事実に関する事項並びに犯罪に関する事項の収集を禁止しており、例外的に審議会の意見を聴いて必要があると認められる場合等にこれらの情報を収集することを可能としている。

(2) これまでの議論の経過

条例要配慮個人情報については、令和4年3月から同年5月までの間にかけて情報公開・個人情報保護審議会小委員会(以下「小委員会」という。)において審議し、さらに同年6月には情報公開・個人情報保護審議会(以下「審議会」という。)においても議論した。その際、区は、全所属への条例要配慮個人情報の該当性調査を行った結果、調査時点では条例要配慮個人情報に該当する情報は存在しないと報告した。

制定に対する前向きな意見が出る一方で、区における事務運用に対する懸念が示されるなど、様々な議論を経た結果、改正法でカバーできる可能性が高い点、実務上具体的な事例が出てきた際に、再度検討して条例を改正することができる点及び条例要配慮個人情報の制定に伴う事務の取扱いが困難となる点、以上の三点の理由により条例要配慮個人情報の制定については見送るべきであるとの結論に至ったところであった。

(3) さらなる議論と審議会としての考え

今般の令和4年10月に設置された小委員会において、区から報告があり、区議会や区民意見提出手続(パブリックコメント)において、LGBTや国籍といった個人情報を条例要配慮個人情報として制定すべきとの意見が複数寄せられたとのことであった。区は、このことを重く受け止め、国の個人

情報保護委員会に対して、区の立法措置として、「世田谷区多様性を認め合い男女共同参画と多文化共生を推進する条例（以下「多様性条例」という。）があることを根拠に、LGBTや国籍といった個人情報を条例要配慮個人情報に制定できるか否か照会したところ、同委員会から、一定程度の情報を条例要配慮個人情報に制定することも妨げられない旨の回答があったとのことである。

こうしたことを踏まえ、区は、総合的に検討した結果、改正法第60条第5項に基づき、国籍、性的マイノリティに関する情報及びドメスティック・バイオレンスに関する情報を条例要配慮個人情報として制定することが適当であると考えに至ったため、再度、審議会に対して意見聴取を行うこととしたものである。

審議会としては、条例要配慮個人情報を制定するにあたっては、多様性条例を根拠とすべきであり、国籍、性的マイノリティ（多様性条例第2条第6号に定める記述）及びドメスティック・バイオレンス（多様性条例第2条第7号に定める記述のうち、改正法第2条第3項に該当しないもの）の三点の個人情報を条例要配慮個人情報として制定することに異議はない。

ただし、区内部における条例要配慮個人情報に関する事務運用等で混乱をきたすことは決してあってはならないため、令和5年4月以降、上記三点の情報を条例要配慮個人情報として適切に取り扱うことができるよう関係所管課と詳細を検討し、適切に職員周知を図ることを求める。また、条例要配慮個人情報の定義の趣旨を鑑み、外部委託、外部提供、目的外利用等を行った案件については、令和4年7月の審議会答申第968号（以下「答申第968号」という。）に倣い、要配慮個人情報と同様に条例要配慮個人情報についても、後述の各審査基準に則った所管課の審査後、審議会に対する報告を求める。

2 個人情報保護管理基準

改正法第66条第1項により、各自治体は、「…保有個人情報の漏えい、滅失又は毀損の防止…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べき義務が生じた。この規定を受け、国から周知された「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」（以下「事務対応ガイド」という。）の指針に則り、各自治体は、安全管理措置を講ずる必要が生じたことから、今般、区は「個人情報保護管理基準」を策定することとしたものである。

審議会としては、区が改正法第66条第1項及び事務対応ガイドに基づき策定した「個人情報保護管理基準（案）」の内容について異議はない。

ただし、今後の区内部での周知を見据えて、改正法や改正条例、当該管理基準等の位置関係が明瞭にわかるよう工夫を凝らすことを要望する。

3 外部委託等の審査基準

現行条例では、区の各所管課は、個人情報を取り扱う業務において外部委託、外部提供、目的外利用等を行う際に、原則として各個別案件ごとに事前に審議会へ諮問し、審議会に承認され次第、業務を開始している。

一方で、改正法では、第66条第1項により安全管理措置に関する基準を示し、外部委託については委託先がこれを遵守することにより、電子計算機への記録及び回線結合については区が安全管理措置を遵守することにより、個人情報の適切な管理が担保されることとなる。また、収集禁止事項及び本人外収集については改正法第61条から第64条までの規定を厳格に遵守し、外部提供及び目的外利用については改正法第69条の規定を厳格に遵守することとなることから、各個別案件の審議会への事前諮問は許容されないところである。

このことを踏まえ、区が前述の「個人情報保護管理基準」を策定したうえで、各所管課が個人情報を取り扱う業務において外部委託等を行う場合に、事前に審査することを可能とする各審査基準を策定するものである。

審議会としては、改正法の枠組みの中、現行条例において事前に審議会へ諮問する事項につき、各所管課が個人情報を取り扱う際に事前審査する審査基準の方向性について異議はない。

ただし、区の所管課が実際に個人情報の保有等を行う場合、その都度、審査基準及び別票を作成し、総括個人情報保護管理者へ提出することとなると、本件に係る事務量が増え、非常に煩雑になることが想定される。よって、各所管課が要配慮個人情報や条例要配慮個人情報を取り扱った場合に限定して総括個人情報保護管理者へ報告することとする等、本件に係る区の所管課の事務負担についても一定程度考慮に入れて検討することが望まれる。

4 開示請求手続の本人確認書類

現行条例施行規則において、開示請求手続の本人確認書類について詳細に定めているものの、改正法が施行される令和5年4月以降は、改正法に基づく開示請求を行うこととなることから、改正法及び政令の規定に沿った対応が求められる。

については、改正法及び改正条例が施行される令和5年4月以降の開示請求手続の本人確認書類については、事務対応ガイドを参考とし、各自治体において具体的な本人確認書類を確定させる必要がある。

審議会としての意見は、以下の三点のとおり。

まず、一点目として、改正法では、開示請求時に確認する本人確認書類について、原則として、開示請求書に記載されている開示請求をする者の氏名及び住所又は居所と同一の氏名及び住所又は居所が記載されていることを求めているため、区がこの方針を採用していることに異議はない。

次に、二点目として、なりすましが特に懸念される任意代理人による開示請求について、現行条例施行規則第10条（開示請求者の確認）において、保有特定個人情報における任意代理人による開示請求の場合に委任者本人の実印を押印した委任状及び当該実印に係る印鑑登録証明書を要求していることから、区がこの対応を継続し、引き続き厳格に対応していくことに異議はない。

最後に、三点目として、本人による開示請求、法定代理人による開示請求及び任意代理人による開示請求の三点の開示請求について、区が提示した各請求時の具体的な本人確認書類は、改正法及び政令並びに現行条例の内容を鑑みた適正な内容であると認められるため、異議はない。

5 死者の情報に関する開示請求基準

現行条例も改正法も「個人情報」は、生存する個人に関する情報であり、死者に関する情報は含まれない。また、改正法では、改正条例に個人情報の定義として死者に関する情報を含める規定を設けることを許容していない。ただし、死者に関する情報が同時に遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報として改正法の保護対象となる。他方、死者に関する情報の取扱いについて個人情報保護制度とは別の制度として条例を定めることは妨げられていないところである。

この点について、答申第968号では、区の個人情報保護制度とは別の制

度としての条例制定は求めないが、条例の運用と同様に内部管理規定により適切な運用を行うべきであるとした。また、現行条例で運用している「死者の個人情報に関する開示請求の取扱い基準」は、ガイドライン等で示されている「死者に関する情報が同時に遺族等の生存する個人に関する情報でもある場合」と同じ主旨と考え、今後、区の開示請求制度が区民にとって後退することがないように、死者に関する取扱い基準を内部管理規定として制定することが相当であるとしたものである。

以上のことから、区は、改正法施行時においても、一定程度の死者の情報も生存する個人が開示請求することを可能なものとする現状の運用を継続するため、審議会に意見を聴いたうえで、「死者の情報に関する開示請求基準」を改めて策定するものである。

審議会としては、区が提示した「死者の情報に関する開示請求基準（案）」は、現行の「死者の個人情報に関する開示請求の取扱い基準」を実質的に継続するものであって現行制度を後退させるものではなく、答申第968号に則ったものであると認められるため、異議はない。

参考 1

諮問第 994 号
令和 4 年 10 月 18 日

世田谷区情報公開・個人情報保護審議会
会 長 山 田 健 太 様

世田谷区長
保 坂 展 人

世田谷区情報公開・個人情報保護審議会条例第 2 条の規定に基づき、下記の事項について諮問します。

記

諮問事項

個人情報の保護に関する法律の改正に伴う世田谷区の個人情報の取扱いに関する運用上の細則等について

諮問理由

個人情報の保護に関する法律（以下「法」という。）の改正に伴う世田谷区における個人情報保護制度等の見直しに向けての考え方については、本年 7 月に世田谷区情報公開・個人情報保護審議会（以下「審議会」という。）の答申として、新たな個人情報保護制度を構築するうえでの「世田谷区の 3 つの基本方針」など、貴重なご意見を取りまとめていただき深く感謝申し上げます。

区としては、答申の内容を踏まえ、本年 9 月に世田谷区個人情報保護条例（以下「条例」という。）の全部改正（素案）として取りまとめ、パブリックコメントを実施したところです。現在、区民から寄せられた意見に対する区の考え方を整理するとともに、改正条例（案）の取りまとめに向けて具体的な運用等の詳細な検討を行っているところです。

つきましては、令和 5 年 4 月 1 日の改正法及び改正条例の施行に向けて、区の個人情報の取扱いに関する運用上の細則等を制定する必要があることから、審議会の意見を聴くものです。

参考2

世田谷区情報公開・個人情報保護審議会委員名簿

氏名	現職等	備考
やまだ けんた 山田 健太	専修大学文学部 ジャーナリズム学科教授	会長 小委員会委員
さいき ひでのり 斉木 秀憲	国土館大学法学部・ 大学院法学研究科教授	副会長 小委員会委員長
つちだ しんや 土田 伸也	中央大学法科大学院教授	小委員会委員
たかやま こずえ 高山 梢	弁護士	小委員会委員
やまべ なおよし 山辺 直義	弁護士 システム監査技術者	小委員会委員
うえだ けいこ 上田 啓子	世田谷区町会総連合会	
おおた まさや 太田 雅也	一般社団法人世田谷区医師会	
あさお まもる 巨尾 衛	世田谷区商店街連合会	
あさくら ひろみ 朝倉 宏美	ひとえの会	
ふじわら かずこ 藤原 和子	世田谷区民生委員児童委員協議会	
よしだ しゅうへい 吉田 周平	元世田谷区立小学校PTA連合協議会	
なかむら しげみ 中村 重美	世田谷地区労働組合協議会	小委員会委員
おおしげ ふみお 大重 史朗	公募委員	
こじま てるお 小島 昭男	公募委員	

(敬称略)

参考3

小委員会の審議経過

- (1) 第1回(令和4年10月26日(水))
 - ・ 条例要配慮個人情報の制定(案)
 - ・ 死者の情報に関する開示請求基準(たたき台)
 - ・ 改正法の安全管理措置に関する基準関係

- (2) 第2回(令和4年11月8日(火))
 - ・ 条例要配慮個人情報の制定(案)
 - ・ 死者の情報に関する開示請求基準(案)
 - ・ 個人情報保護管理基準(案)
 - ・ 外部委託等の審査基準(案)
 - ・ 開示請求手続の本人確認書類(案)