資料１-３

世界経済フォーラム第四次産業革命日本センター

World Economic Forum
Centre for the Fourth Industrial Revolution Japan

目次

資料１-３

G20 Global Smart Cities Alliance

１．G20 Global Smart Cities Allianceについて

G20 Global Smart Cities Alliance

Goal

テクノロジーの社会実装に必要なルール作りや合意形成（テクノロジーガバナンス）に関して、都市や自治体のサポート役となり、スマートシティの実現に貢献する。

Impact

- G20 Global Smart Cities Allianceとして、都市ネットワークの知見を集約し、テクノロジーガバナンスに関するリファレンス先としての地位を強固にする。
- プライバシーやセキュリティ、排他的なデータ利用や、ベンダーロックイン、都市間のインターオペラビリティといった諸問題を回避すべく、パイロット都市と共に、スマートシティに関する基本原則を共同設計する。
- Allianceの活動を通し、各都市間で情報が共有される事で各都市が過剰な投資を行うことなく、市民にとって最も価値ある選択が行う事が可能となる。

Partners

日立, NEC, エーザイ, Salesforce, NTT, 森ビル, Deloitte Touche Tohmatsu Limited, MURC

Timeline

2018年秋-2019年春：スマートシティをG20の議題に盛り込む点につき日本政府の合意を得る。既存の活動と矛盾・重複しない形で、国際コンソーシアムの創設に向けた調整を行う。

2019年春～夏：B20, U20, G20を通し、Global Smart City Coalition創設について支持を得る。

2019年夏～秋：Asia Smart City Weekにて、G20 Global Smart Cities Alliance 設立会合を実施

2019年秋～冬：バルセロナのSmart City Expo及び、Innovative City Forumにて自治体や政府関係者、スマートシティ関係のエキスパートを招いたテクノロジーガバナンスに関するワークショップを開催

2020年春～夏：5原則に基づく各ポリシーの策定を専門家と共に開始。日本においては日本支部として10都市以上が参画

2020年秋～冬：U20サミットへの参画の他、Smart City ExpoにてGSCA1周年記念イベントを開催予定

CONTACT:
Jeff.Merritt@weforum.org;
Rushi.Rama@weforum.org
Yuta.Hirayama@weforum.org;

１．G20 Global Smart Cities Allianceについて

2019年10月の設立会合では、トロント市やバルセロナ市等各都市より、スマートシティに関する取り組みや、テクノロジーガバナンスついての議論が行われた。また、サウジアラビア政府より、来年度のG20議長国として、G20 Global Smart Cities Allianceの取り組みを引き継いでいく旨の発表も行われた。

資料１-３

１．G20 Global Smart Cities Allianceについて

G20 Global Smart Cities Alliance

2020年のG20デジタル経済大臣会合の成果文書に本年もG20 Global Smart Cities Allianceの活動について明記されました。


G20 Digital Economy Ministers Meeting

Ministerial Declaration

G20

III. Smart Cities

12. Building on the achievements of past Presidencies, we encourage further work with stakeholders for the development and deployment of digital technologies and solutions for human-centric, environmentally sound, sustainable, rights-respecting, and inclusive smart cities and communities that boost competitiveness and enhance well-being and community resilience. These digital solutions should be centered around connectivity and providing services in more efficient and personalized ways, while safeguarding human rights. These digital solutions should also be deployed responsibly with effective security and resilience in the digital economy to safeguard privacy, personal data, and service provision, and foster greater transparency and public trust. In this respect, we take note of the G20 Global Smart Cities Alliance initiative launched in 2019.

１．G20 Global Smart Cities Allianceについて

G20 Global Smart Cities Alliance

本アライアンスでは、都市ネットワークと協力し、20万以上の都市および地方自治体、世界のリーディングカンパニーやスタートアップ、研究機関・市民社会コミュニティと「スマートシティにおける５つの原則」を中心に、「テクノロジーガバナンスの実現」と「都市間のガバナンスギャップ解消」に向けた議論を加速させていく。

設立パートナー一覧: ※都市ネットワークとの連携は今後も順次拡大予定

G20 2019 JAPAN / G20 Saudi Secretariat / Smart City / ICLEI Local Governments for Sustainability / World Economic Forum / ITU / UCLG United Cities and Local Governments / SMART CITY EXPO WORLD CONGRESS / Open & Agile Smart Cities / CATAPULT Connected Places / cigf / C40 CITIES FOR ALL Global Compact on Inclusive and Accessible Cities / What Works Cities / Results for America / World Enabled / OSCN cigf Commonwealth Sustainable Cities Network / CitiesToday Institute / Digital Future Society / Smart City Institute Japan / Leading Cities / WeGO / G3ict / 伏義智庫 Fuyi Institution

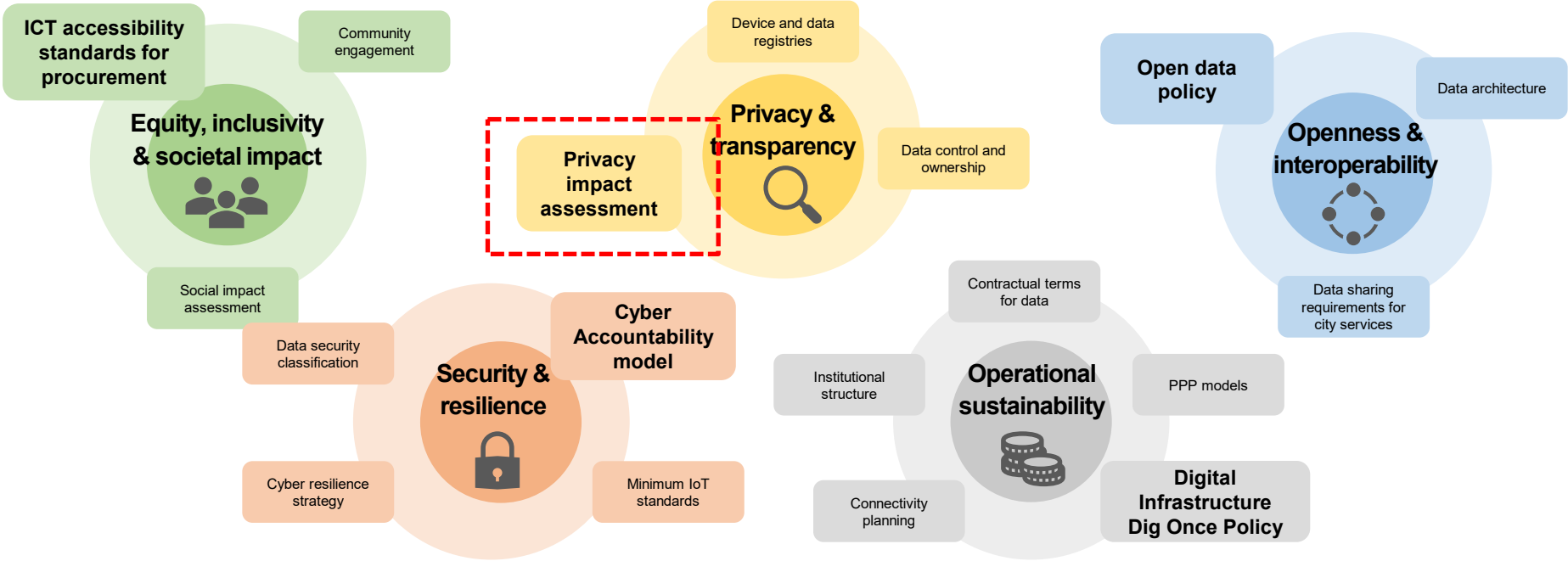
【スマートシティにおける５つの原則】

- Safety, security & resiliency
- Transparency & Privacy
- Interoperability & openness
- Equity, inclusion & societal impact
- Operational & financial sustainability

１．G20 Global Smart Cities Allianceについて

G20 Global Smart Cities Alliance

倫理的なスマートシティ構築のための5つの原則およびポリシーフレームワークに沿った個別ポリシー策定を目指し、セキュリティやオープンデータといった領域にてドラフトポリシーの策定を開始。本日はそのうちの一つであるPIAポリシーについて紹介します。



資料 1 - 3

Introduction to

Privacy Impact Assessment Model Policy

G20
Global
Smart Cities
Alliance

プライバシーインパクトアセスメント モデルポリシーの構成

本書の構成

Objectives / 目的

Foundations for Privacy Impact Assessments / PIAの基本要件
1. Organizational Values and Risk / 組織の価値観とリスク
2. Scope and Timing / 範囲とタイミング
3. Tools and Components / ツールと構成要素
4. Roles and Responsibilities / 役割と責任
5. Monitoring and Recordkeeping / 監査と記録
6. Transparency & Engagement / 透明性とエンゲージメント

Fundamentals of a Privacy Impact Assessment / PIAの構成要素
Additional Guidance & Resources / 追加情報
Acknowledgements / 謝辞

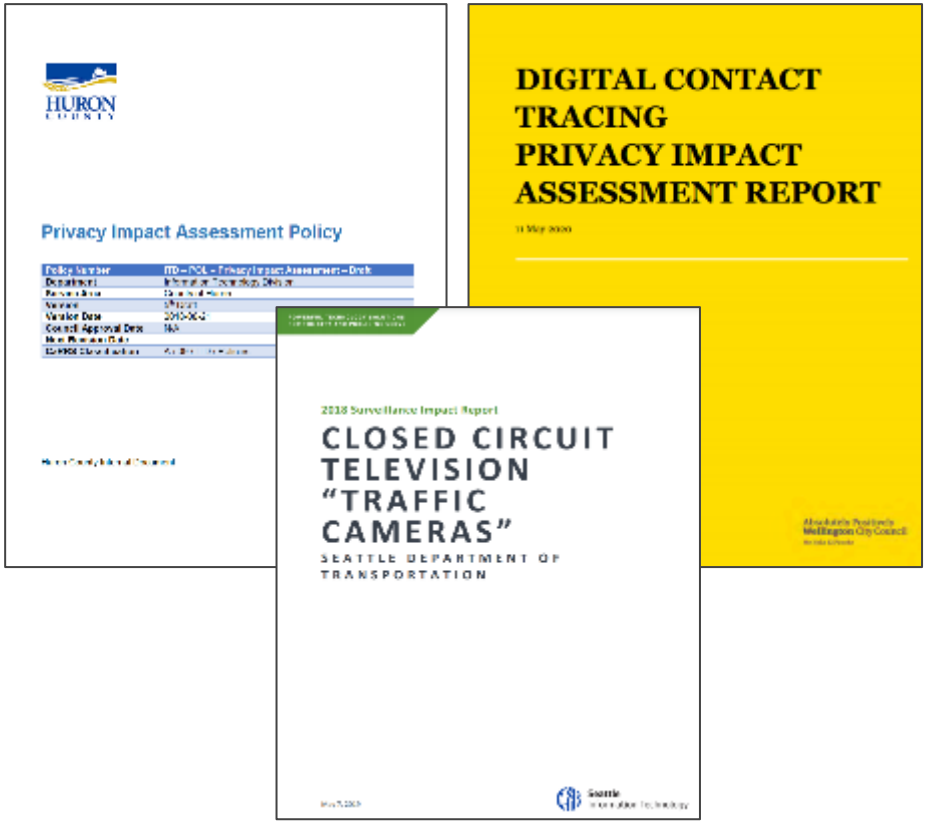
G20 Global Smart Cities Alliance

２．プライバシーインパクトアセスメントとは何か?

プライバシーインパクトアセスメント (PIA)は、特定の情報システム、テクノロジー、またはプログラムによって個人情報がどのように収集、使用、共有、および維持されるかを評価するものです。

*PIA*は、以下にも含まれます:

- Data Protection Impact Assessments (DPIAs) - EU GDPR https://gdpr-info.eu/issues/privacy-impact-assessment/
- Surveillance Impact Assessments or Reports (SIAs, SIRs)
- Algorithmic Impact Assessments (AIAs)
- Ethical Impact Assessments (EIAs)
- Human Rights Impact Assessments (HRIAs)



G20 Global Smart Cities Alliance

３．PIAポリシーの重要性について

本モデルポリシーは、倫理的な意思決定をサポートし、個人およびコミュニティに対するプライバシーリスクを最小限に抑えることにより、イノベーションを促進します。

- 透明性と説明責任を通して、市民の信頼を築きます
- 予測可能なプライバシーの害またはさまざまな影響を軽減します
- コンプライアンスを改善し、法的リスクを軽減します
- 市全体のデータとテクノロジーに関するより自信を持って一貫した意思決定を可能にします

G20 Global Smart Cities Alliance

４．本モデルポリシー実装のメリット

本モデルPIAポリシーは、プライバシーとデータの保護に関する基本的な考え方を提供します。
プライバシーリスクを可視化するために従うべきプロセスと考慮すべき観点を提示しています。

- PIAは、今や世界のいたるところで、官民双方にとってベストプラクティスもしくは、法的要件となっています。
- 本ポリシーは新しいテクノロジーを実装する前に潜在的なプライバシーリスクへの対処となります。
- 本ポリシーは、地域の優先順位とリソースに応じて柔軟に対応が可能です。
- 本ポリシーは、倫理的なスマートシティ5原則の他の原則(公平性や、包括性など）にも貢献します。
- このポリシーの実装による、データ資産の可視化、プライバシー原則の策定、一般市民の関与といった副次効果の実現も期待できます。

資料１-３

G20 Global Smart Cities Alliance

５．本モデルポリシーの主な構成

How and when to do PIAs
PIAをいつどのように実施するか

Foundation of PIA / PIAの基本要件

- 組織の価値観とリスク
- 範囲とタイミング
- ツールと構成要素
- 役割と責任
- 監査と記録
- 透明性とエンゲージメント

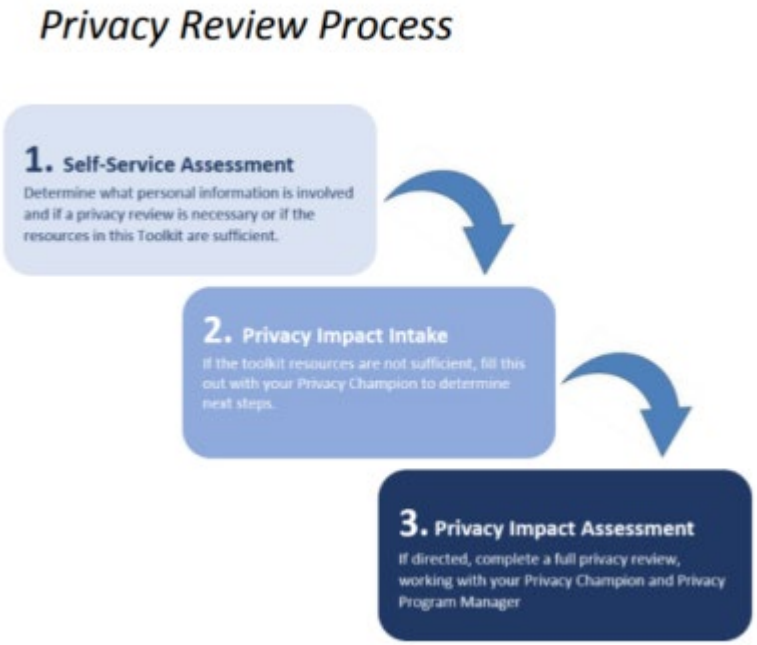
What's in the PIAs
PIAには何が含まれているか

Fundamentals of a PIA / PIAの構成要素

- 技術/データプロジェクトの詳細
- 潜在的なプライバシーリスク
- 潜在的な便益
- データ利活用および管理方針と、
  その他の保護手段
- 追加の要因とコンテキストの考慮事項

G20 Global Smart Cities Alliance

６．シアトル市の事例（ご参考）



City of Seattle – Department of Information Technology

City of Seattle Privacy Program

October 2015

①セルフサービス評価
プライバシー評価の最初のステップとして、評価アンケートを実施する。プライバシーリスクが低い場合は、市のプライバシー条件を満たせるようツールキットを活用し、プライバシー保護を実施する。

②プライバシー閾値分析
プロジェクトのプライバシーリスクが高いと判断された場合は、プロジェクトオーナーはプライバシーに関する追加の質問を受けプライバシーに関する閾値分析を実施します。部門のプライバシー責任者は閾値分析を確認し、プロジェクトオーナーがプライバシーリスクを軽減するためのツールを提供するか、必要に応じより詳細なプライバシーレビューを実施します。

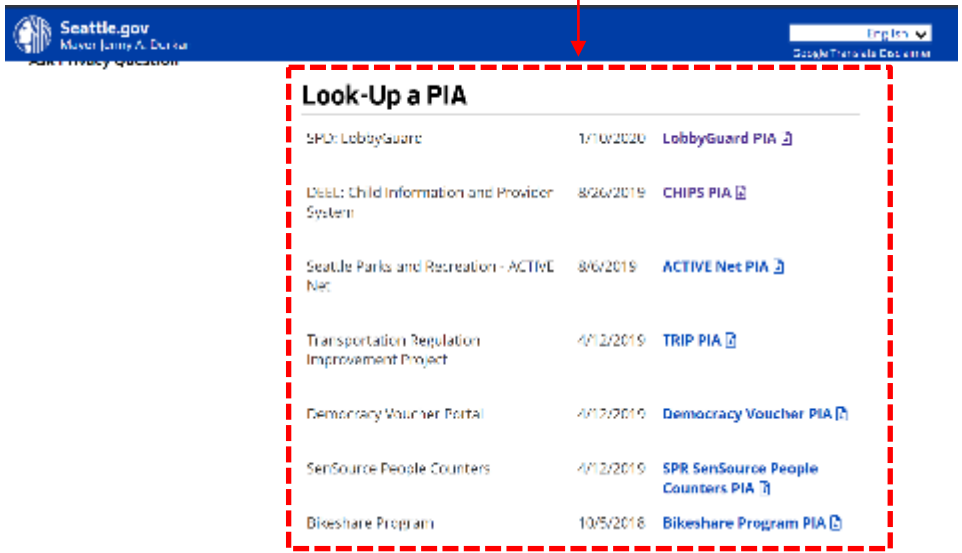
③プライバシーインパクトアセスメント
プロジェクトまたはプログラムに、重要なプライバシーリスクがある場合、プロジェクトオーナーはプライバシー影響評価（PIA）の完了を求められます。このドキュメントはプロジェクトまたはプログラムを詳細に調べ、プライバシーへの潜在的な影響と緩和オプションをすべて決定するため、一定の時間を要します。

（出典：シアトル市のプライバシープログラムを参考に記載）
http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf

G20 Global Smart Cities Alliance

６．シアトル市の事例（ご参考）

シアトル市では、それぞれのプロジェクトごとにPIAを実施、公開し、どの程度PIAが閲覧されているかも含め公開しています。



資料１-３

７．PIAポリシーの実装に向けてどこから始めるか

G20 Global Smart Cities Alliance

G20 Global Smart Cities Allianceでは、36のパイオニア都市と実装に向けた以下の取り組みを推進しています。

モデルポリシー実装に向けたステップ:

- 各都市における現時点の法令や、プライバシー保護に関する取り組みとのギャップを認識します。
- PIAを進めていくチームを組成します。
- 一つのプロジェクトを選び仮説検証を行います。
- ワークショップを実施します。
- 各地の実情に合わせ、モデルポリシーを調整し、その都市のPIAポリシーとして実装します。

その他参考になる事例:

- Wellington
  digital contact tracing PIA
- Seattle
  privacy reviews & surveillance reviews
- Toronto
  PIA Policy
- Helsinki
  Data Protection Tools

Model Policy

Privacy Impact Assessment

G20 Global Smart Cities Alliance

本モデルポリシーは G20 Global Smart Cities Alliance の基本原則である Privacy & Policy に属する一つのポリシーです。本ポリシーの実装に伴う補完的な情報については、GSCA のウェブサイトにも記載をしています。

Background

世界中の都市は驚異的なスピードで成長しており、経済的な機会や快適さを求める住民が集まっています。市政府は、市民中心のサービスを可能にするテクノロジーや「スマートシティ」ソリューションを導入し、より持続可能で、包括的で、開かれた都市へと発展させることで、その継続的な成長に対応しています。これらの目標を達成するためには、あらゆる規模の都市とコミュニティが、これらのテクノロジーによって生成された個人とコミュニティに関するデータが適切に保護され、保護されていることを確認しなければなりません。

データの収集は、公共料金の支払いからウェブページの閲覧、市道を歩く姿や、公共交通機関の利用、自動車の運転といった様々な日常生活をサポートする都市運営の中で行われています。例えば、センサーやコネクテッドデバイスが常時接続され、データが流れることで、交通システムの管理や、公共インフラ全般におけるリアルタイムメンテナンス、全自動の公共サービス、透明性のあるガバナンスとオープンデータの実現、公共エリアでの救急サービスのサポートなど、スマートテクノロジーの利用は行政と市民の双方に便益をもたらします。たとえ、これが善意の取り組みであったとしても、個人のプライバシーを侵害するリスクを生み出し、監視への恐れを高めることによって都市生活の利点を否定し、個人が公共空間に関わることへの阻害にも繋がりかねません。

新たに台頭したテクノロジーやビジネスシステム、法律や規制の変化と複雑化、さらには世間の注目を浴びるようになったことから、都市は、プライバシーとデータ保護を積極的かつ体系的に活動に組み込むための適切な措置を講じることが求められています。プライバシーは、伝統的に、さまざまな権利を包含するより広い概念として理解されている一方、データ保護とは、個人データの収集、使用、処理に関連し、個人を保護することを意味します。

都市は、事業を遂行するためにデータを利用・共有するという自らの必要性と、より広範な公共の福祉や個人のプライバシーの利益との間で、公共の信頼を構築し維持する方法でバランスを取らなければなりません。市民の信頼が得られなければ、スマートシティ技術の恩恵を享受し続けることはできません。都市は、個人、地域社会、技術提供者が責任を持ってデータを利用することで、個人や地域社会のプライバシーリスクを最小限に抑えながら、その恩恵を最大限に享受できるような政策と実践に投資しなければならないのです。

プライバシー影響評価（PIA）ポリシーを実施することで、都市はプライバシーリスクを特定、評価、対処するための一貫した方法を確立することができます。世界各国では、プライバシーやデータ保護に対する文化的・法的なアプローチに大きな違いがあるため、モデルとなる PIA ポリシーを作成するのは複雑な作業となります。本ポリシーでは、従うべきプロセスと考慮すべき問題点を規定することで、都市がより自信を持って、地域社会の期待に沿った形でプライバシーリスクを検討し、対処する可能性を高めることができると期待しています。

Contents / コンテンツ

Model Policy / モデルポリシー

Objectives / 目的

市は、必要なサービスを提供するために情報を収集することと、特に革新的なスマートシティ技術を導入する場合には、市民のプライバシーを保護することとの間に公正なバランスを見出すように努めなければなりません。プライバシー影響評価（PIA）は、不可欠なプライバシー評価ツールです。PIA は、収集から廃棄に至るまでのデータのライフサイクル全体を通して、プライバシーリスクを特定し、管理するための一連のプロセスで構成されています。スマートシティにおける技術の取得や使用に先立って PIA を実施することは、透明性と説明責任を高め、市民の信頼を支え、潜在的なプライバシー侵害を回避し、コンプライアンスを改善して法的リスクを軽減します。PIA の実施によってデータや技術に関し、市職員、そのパートナー、市民による、より確かで一貫した意思決定を可能にすることができます。

市の PIA ポリシーは、プライバシーリスクの特定と軽減において、対処すべき問題と従う

べきプロセスを特定すべきです。具体的には、PIA ポリシーは、以下に留意する必要があります。

- PIA ポリシーはデータと技術の具体的な目的、潜在的なプライバシーリスクと軽減策を明確にし、市と地域社会の価値観、優先順位、法的権利と照らし合わせて評価すべきです。
- PIA ポリシーは、プロジェクト全体とデータのライフサイクルとが一致している必要があります（これには、部門を超えて発生する調達、データセキュリティ、アクセシビリティ、公的記録に関する事が含まれます）。
- PIA ポリシーは、特定の時点で「個人」または「個人を特定できる」と見なされるデータだけでなく、テクノロジーまたはサービスによって収集されるすべてのデータに対処する必要があります。
- PIA ポリシーは個人情報の取り扱いに関する社内外のコミュニケーションと協力を促進し、市が特定の技術への再考や、地域社会、パートナー、技術提供者に通知する際に、明確な理解が得られるようにします。
- PIA ポリシーは、個人のプライバシーや社会全体への悪影響を最小限に抑えつつ、倫理的な意思決定を支援し、データの有益な利用を最適化することで、イノベーションを加速させます。
- [より参加型のオプション]: データとテクノロジーの実践に関する市民の参加と意思決定のために、ワークショップや集会など、多様な機会を設けることも重要です。

Examples（具体的な事例）：

- http://www.longbeach.gov/globalassets/health/healthy-living/office-of-equity/clb_toolkitbook_singlepages
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Foundations for Privacy Impact Assessments / PIA の基本要件

本セクションでは、PIA ポリシーの具体的な目標である、個人および地域社会の社会的利益を最大化し、リスクを最小化するという全体の目的を達成するための基本的な構成要素について記載します。

1. Organizational Values and Risk / 組織の価値観とリスク

a. 都市は、PIA プロセスにおいて、特定の技術やサービスが評価される際の公共の価値、優先順位、プライバシーの原則を明示的に示すべきである。

> **Examples:**
> - NYC's IOT Guidelines
> - Seattle's Privacy Principles
> - Barcelona's Digital Service Standards
> - India's Data Smart Cities Strategy

b. 市は、PIA プロセスにおいて特定の技術やサービスが評価される際の法的基準や権限、既存の市の方針や原則を明確に示すべきである。

c. PIA は、リスクと利益を評価する際には、倫理、公平性、行政による関与など、法令遵守以外の考慮事項を考慮に入れるべきである。これらの考慮事項には、個人への影響だけでなく、グループへの影響も含まれるべきである

d. [より高い成熟度のオプション]: PIA プロセスには、上記で特定された価値観に基づいて算出されたスコアリングモデルの適用を含んでも良い。

> **Examples（具体的な事例）:**
> - https://wellington.govt.nz/~/media/about-wellington/emergency-management/files/covid-19/wcc-privacy-impact-assessment-digital-contact-tracing.pdf?la=en

e. [より参加型のオプション]: 市の職員や、市民、特に社会的弱者を巻き込み、広範な市民の価値観、原則、リスクのしきい値を決定する。モデル化においては、市民協議会、市民ボランティア活動、市民集会等の議論や、市財政や予算編成における電子投票、草案の公開注釈、ソーシャルメディア等の活用を含む。

2. Scope and Timing / 範囲とタイミング

a. 初期評価（または完全な PIA の必要性を判断するための他のしきい値分析）は、以下のタイミングで実施すべきである。

i. あらゆる新技術の開発又は調達において、可能な限り早期に実施する。［具体的には、プライバシー保護を調達基準や開発クライテリアに組み込む事を含む］。設計・実装後にプライバシーリスクを低減するためのシステム改修を行うことは、よりコストがかかることが証明されている。

ii. 既存のプロセスやシステムの重要な変更を計画する場合に実施する。これには、新たにデータ活用を行う場合や何らかの変更といったプロジェクトが更新されたタイミングを含む。

b. 市の規則や政策で要求されている場合、または初期評価で以下のように判断された場合には、完全もしくは部分的な PIA を実施すべきである。:

i. 個人を特定する可能性のあるデータのための新しい技術、新しい目的、または新しいプロセスが導入される場合。

ii. システム内の他の情報と個人情報との物理的または論理的な分離に影響を及ぼす可能性のある方針、業務プロセス、またはシステムの大幅な変更が計画されている場合。

iii. 機密性の高いデータが処理される場合、または技術やサービスにより高リスクのデータ処理が可能になる場合［例えば、個人のスコアリング／プロファイリング、系統的なモニタリング、大規模処理、複数のソースからのデータのマージまたはマッチング、子供または社会的弱者をターゲットとしたもの、身体的危害のリスク、または新しい技術の使用や既存技術の新規適用など］

iv. 技術またはシステムが自動的もしくは半自動的に、個人に対し、影響を及ぼすような意思決定を行う場合。

c. 必要に応じ、データ収集が可能となる技術を、市内に実装する前に、もしくは市の意思決定プロセスに実装する前に、PIA を実施すべきである。

d. PIA は、収集時に 法的に「個人的」または「個人を特定できる」とみなされるデータが収集されるときだけでなく、技術やサービスによって収集されたすべてのデータを評価するために実施すべきである。

e. PIA は包括的なプライバシープログラムの一部に過ぎないため、データを収集しないこと、プライバシー保護に関する技能訓練、規制、各地方自治体や当局の方法の中での PIA の監査と公表といった各種の取り組みを並行して行うべきである。

3. Tools and Components / ツールと構成要素

a. 市は、完全な PIA [または非個人データの倫理的影響評価]の完了など、さらなる検討が必要かどうかを明らかにするために、予備的な初期評価またはその他のしきい値分析を策定し、実施すべきである。

b. 初期評価では、システム、製品、またはサービスによって引き起こされるプライバシーリスクの初期評価が行われるべきである。これには、詳細なデータフロー図や、予備的なデータと使用特性等が含まれる。

> **Examples（具体的な事例）：**
> - Helsinki Initial Assessment
> - Seattle's PIA Policies
> - Toronto's PIA Policies

c. 完全な PIA が必要であると判断された場合、その完全な PIA は以下の点が含まれるれるべきである（下記の「PIA の基礎」を参照）。

i. プライバシーリスクの評価 - プライバシーリスク評価を実施することで、システム、製品、またはサービスに起因するプライバシーリスクを特定し、それらに優先順位をつけて、リスクへの対応方法について十分な情報に基づいた意思決定を行える。

ii. リスク対応の決定 - 評価されたリスクにどのように対応するかを決定する際には、都市は組織の価値観とリスク許容度の決定を参考にすべきである。対応方法としては、以下のようなものが含まれる。

- **軽減**（リスクは、データの最小化などの技術的・政策的措置により、許容可能なレベルにまで下げることが可能）。
- **移転/共有**（リスクは契約や保険などにより他の当事者と共有される。同意取得は、個人のリスク共有の形態の一つであり、個人は、その情報の提供に関して同意を求められる前に、関連するリスクがどういうものか合理的に理解可能となる）。
- **回避**（都市は、リスクが便益を上回る場合には、特定の技術を使用しないことを選択したり、 特定の種類のデータ処理を行わないことを選択したりできる）。
- **保有**（都市は、悪影響の可能性や影響が低く、利益が大きい場合には、リスクを受け入れることを選択できる）。

iii. 市が設定すべき要件と管理権限

- **法的義務の適用**（組織としてのプライバシーに関する要求事項は、市が遵守する法令、 プライバシーに関する価値観および政策を示す手段である。組織としてのプライバシーに関する要求事項は、法的環境（例えば、法律、規制、方針、文化的価値観、関連する基準、

プライバシー原則など）やリスク低減が可能と判断されたリスクなど、様々なものから導き出されます。

- **軽減可能なリスクへの対処**

d. 市は、PIA の実施およびプライバシーリスクの評価のための専門的なガイダンス、テンプレート、ツールについて、各地のデータ保護当局やその他のプライバシーおよびデータ保護の専門家に相談すべきである（下記の追加ガイダンスを参照）。

> PIA を実施するにあたって確実な方法は、最初にワークショップを行う方法であり、必要なすべての利害関係者によって行います。責任の割り当ては、最初の会議で行われます。最初の会議の後に行う、影響評価に関するワークショップ（複数回になる場合があります）では、専門家は事前に担当範囲についての整理をしておきます。なお、データの文書化をツールにしていく作業は、共同で行うことができます。

4. Roles and Responsibilities / 役割と責任

a. チーフ/シティ・プライバシー・オフィサー（CPO）などの指定された上級職員（必要に応じて専任のプライバシー・チームのサポートを受ける）は、以下の点について責任を負うべきである。

i. 市の初期評価と PIA ツールのための適切なテンプレート、リソース、コンポーネントの開発

ii. PIA の実施に関する基準と実施に伴うリソースの資格要件を設定すること

iii. 初期評価の見直し、またはその他 PIA が必要な場所を決定すること（既存の PIA の再検討を含む）。

iv. プライバシーへの影響を緩和するための要件や勧告を提供することを含む、PIA の実施と承認を行うこと。

v. PIA の過程で提起されたプライバシー及びセキュリティ上の懸念を解決するために、他の関係者と連絡を取り合うこと。

vi. 特定されたプライバシーリスクに対する市の対応を決定すること。

b. 庁/部局/プログラム担当者は以下の点について責任を負うべきである

i. 提案された技術とその利用に関する適切な情報と文書の提供（例：技術の機能性、ビジネスケース、提案された目的、継続的なプライバシーとセキュリティ保護のためのコストなど）。

ii. 初期評価の実施、および必要に応じた完全な PIA の実施の支援。

iii. 提案された技術に関連するリスクを軽減するために、必要に応じて、PIA で特定されたデータの利用及び管理計画、並びにすべての適切な保護措置を実施すること。

iv. PIA の方針が職員に伝達され、職員が PIA プロセスに参加するための十分な時間と資源が与えられていることを確認すること。

v. プライバシーに影響を与える可能性のある技術の使用に先立ち、必要に応じて PIA を認可し、承認すること。

c. 市長や最高技術責任者などの幹部または上級職員は、以下のような PIA ポリシーの遵守を監督する権限を持つべきである。

i. PIA ポリシーが全職員に伝達され、実施されることを確認する。

ii. プライバシーとセキュリティ要件を尊重しつつ、情報が可能な限り共有され、アクセスできるようにすること。

iii. 指定されたプライバシー担当上級職員及びその他の職員が日常的に PIA を実施できるように、適切な予算及び組織構造を提供すること。

iv. 適切な説明責任措置（例えば、エスカレーション手順、スタッフの研修と認識、報告システム、プライバシーに関連した苦情や潜在的な脅威の受け付けなど）を開発し、実施すること。

v. PIA ポリシーの有効性と成果を監視すること

vi. スマートシティプロジェクトのスケジュールと PIA のスケジュールの整合性を見直すこと。

d. 特定の技術やサービスの性質を考慮して、必要に応じ、以下のような追加の市職員や外部の利害関係者に相談すべきである。

i. PIA プログラムに助言し、各部局の参加を促すことができる市幹部や市議会議長等の代表者

ii. 技術システムの設計、データセキュリティリスクの評価及び軽減を支援する CISO 又はその他の IT 専門家

iii. 適用されるデータ保護規則を含む法的基準の遵守を確実にするための、市の弁護士または法律顧問

iv. データが開示される範囲を明確にするための（意図的にまたは法律で）公的記録に関する担当者とオープンデータに関する担当者

v. 調達担当者

vi. データまたは技術に関し別の視点をもたらす他都市の公務員

vii. 特定分野の外部専門家

viii. 技術パートナー

ix. 影響を受けるコミュニティのメンバー

e. [より成熟したオプション]: 上級プライバシー担当者は、データ保護、リスク管理、セキュリティの専門家によってサポートされ PIA を実施する。データプライバシーチームは、市全体のプライバシーチャンピオン（PIA プロセスを支援する特定分野の専門家）ネットワークによってサポートされ PIA の実施プロセスを支援する。PIA チームは、組織の知識とベストプラクティスを構築し、市全体でより一貫性のあるプライバシーの意思決定をサポートし、PIA のプロセスと結果を改善する機会を明確にする。

Examples:
- Toronto RMIS w/in I&T division
- Seattle privacy champions

Examples(具体的な事例):
- Seattle Surveillance Working Group
- Oakland Privacy Advisory Commission

f. [より参加型のオプション]: 外部の機関または組織が、意見、勧告、コミュニティの専門性の活用、または PIA 実施の承認を行うために従事する。このグループには、プライバシーやデータ保護の専門家やコミュニティのメンバーなど、多様な利害関係者の代表者が含まれる。

5. Monitoring and Recordkeeping / 監視と記録

a. すべての初期評価と PIA は、書面で完全に文書化され、市の記録保持の規則に従って維持されなければならない。

b. PIA レビューの結果、除外されると判断された技術も、記録され、文書化されなければならない。

c. もし市に複数の PIA がある場合は、PIA を種類に応じて分類することができる。

d. 地方自治体は、かつては個人を特定できないと考えられていたデータが時間の経過とともに個人を特定できるようになるのを防ぐために、[3 年に 1 度] 程度、IoT テクノロジーまたはサービスによって生成されたすべてのデータを一緒に評価することで、都市は将来に渡りより確かな評価ができるよう、 PIA プロセスの見直しまで含めた運用を策定すべきである。

e. 個人情報保護のために指定された上級職員は、PIA ポリシーを毎年（必要であればそれよりも早く）見直し、必要に応じて更新すべきである。

f. 市の部局、課、プログラム、およびパートナーやサービス提供者は、PIA 方針の遵守度を評価すべきである [内部監査、プログラムレビュー、またはプログラム評価の実施など]

g. 市がプライバシーに関する苦情を受けた場合や、プライバシー侵害が発生した場合には、プライバシー担当の上級職員が調査を行い、必要に応じて状況を改善する。

h. [より成熟度の高いオプション]:都市は、データを処理するシステム／製品／サービスの目録を作成し、維持するべきである。これには、システムやその構成要素に関する所有者や運用の役割、データの出所、発明されたシステムのデータアクション、データアクションの目的、データ処理環境が記載される。

Precedents:（先行事例）

- Seattle's inventory of surveillance tech
- Amsterdam's IoT Registry
- Barcelona's Sentilo
- City of Boston's pilot of Digital Transparency in the Public Realm
- NIST privacy framework

6. Transparency & Engagement / 透明性とエンゲージメント

a. 可能な限り、都市は、すべての PIA を、アクセスしやすく、外部に向けたウェブサイトで公開すべきである。

> **Precedents:** （先行事例）
> - Seattle PIA and SIR inventory
> - Wellington DCTT PIA

b. 市は、組織や個人がデータの処理方法や関連するプライバシーリスクについて信頼できる理解を持ち、対話を行うことができるよう、適切な活動を開発し、実施すべきである。

c. 都市は、スマートシティ技術に関連したデータ処理の目的、慣行、プライバシーリスクを、関連する PIA に基づいて知らせるための仕組み（通知、内部報告書、公開報告書など）を開発すべきである。

d. [より参加型のオプション]: データ処理および関連するプライバシーリスクに関する個人からのフィードバックを得るための仕組み（調査やフォーカスグループなど）が確立され、実施される。

> **Supplementary guidance（追加ガイダンス）:**
> - PIA では、頭字語、スラング、または外部の聴衆にあまり知られていないその他の用語の使用を避ける必要があります。さらに、回答は、トピックに不慣れな聴衆がアクセスできるように、主に非技術的な言語を使用して作成する必要があります。
> - サイネージは、関連する地域のプライバシー規制に準拠するために、必要に応じてその場で提供する必要があります[また、データの収集および処理活動を一般に知らせるために、IoT テクノロジーの新規または新規の展開を検討する必要があります]。

Fundamentals of a Privacy Impact Assessment / PIA の構成要素

このセクションでは、データとテクノロジーによる公共の利益を最大化しながら、都市とそのパートナーが潜在的なプライバシーリスクを効果的に特定、軽減できるようにするため、PIA で取り組むべき基本的な問題や疑問点を説明します。

PIA は、以下で説明するように、明確で分かりやすい必要があります。

1. テクノロジーの使用や説明責任を負う対象である、市の部局やプログラム、パートナーやサービス提供者を特定すること。

2. 設計または取得するテクノロジーについて、それらの一般的な能力や機能、生成される可能性が高いデータの種類、収集された個人情報のソースと正確性の説明について記述すること。（市の部局が提案した用途以外で合理的に予測可能な監視能力を含む）

3. 個人やコミュニティ、社会一般に対する想定価値や便益（それらを証明するデータや研究）を含む、テクノロジーの目的や利用案を記述すること。テクノロジーが解決しようとしている問題や、侵害性の低い代替技術の有無についても記述すること。

4. 必要に応じて、提案されたテクノロジーに関する個人データを収集、利用、開示するための市の権限を記述すること。

5. テクノロジー評価が行われている、公共の価値や原則、法的基準、組織的リスクフレームワークについて記述すること。

6. 提案されたテクノロジーの使用に関する潜在的なプライバシーリスクを評価、記述すること（リスクが発生する可能性や個人、コミュニティへの潜在的な影響の重大性を含む）

7. 組織の価値観とリスク許容度 [リスクの軽減や移転・共有、回避、受容など]を踏まえて、特定されたリスクへの市の対応を記述すること。

8. 提案されたテクノロジーの利用について、以下のような、明確な利用方針とデータ管理ポリシーを記述すること。:

    a. テクノロジーがいつ、どのように提供され、使用されるか、誰によって行われるか（必要に応じ、誰がどのような条件で、データの所有権やライセンス権を持つのかの記述を含む）.

    b. テクノロジーを統制する追加の規則（犯罪捜査目的など、テクノロジーを使用する前に満たすべき法的基準を含む）.

    c. データをどのように安全に保存し、破棄、非識別化するか.

    d. データが識別可能、識別不可能な形態で、どのくらいの期間保持されるか

    e. データへのアクセスをどのように監視および管理するか（アクセスログや監査を含む）

f. 技術やデータを共有するかどうか、共有する場合はどのような条件か（パートナーやサービス提供者、他の政府機関、研究者、公文書要求、オープンデータなどの日常的な共有と、緊急事態の場合の両方を含む）

g. テクノロジーを扱い、データにアクセスする全ての職員が、市のポリシーを遵守してテクノロジーを使用することを保証するため、どのようなトレーニングと説明責任の施策を行うのか

h. データの機密性、完全性、可用性を確保するために、どのような保護策があるか（ランサムウェアやマルウェア、IoT 脆弱性などの脅威からの保護を含む）

i. テクノロジーの使用に関する潜在的なプライバシーリスクの軽減を目的とした、その他の法的、組織的、物理的、技術的な保護策

9. 実施された地域活動と今後の地域活動計画、受け取ったコメントと市の回答、テクノロジーの取得と使用から生じる可能性のある近隣住民への影響と差別的効果についての市の結論を記述すること。

10. データの使用方法やデータの管理プロセスを変更する可能性のある、緊急事態や防衛上の理由についても記述すること。

11. テクノロジーによる、市民の権利と自由に与える潜在的な影響と、社会的弱者への潜在的な差別的効果の影響が、どのように考慮、軽減されるかを記述すること。

12. テクノロジーの運用に関するプライバシーおよびデータ保護の維持コスト（人件費、法令遵守、監査、データ保持、セキュリティコストなど）のための資金調達ついて記述すること。

Additional Guidance & Resources / 追加情報と資料

Examples of City PIAs / 各都市の PIA ポリシー

- Helsinki Data Register and DPIA tools
- Huron County Privacy Impact Assessment Policy
- Santa Clara County Surveillance Use Policies
- Seattle PIA Reviews and Surveillance Reports
- Toronto Privacy Impact Policy
- Wellington Digital Contact Tracing PIA

Guidance on conducting a PIA or DPIA / PIA と DPIA 実施ガイダンス

- The former Article 29 Working Party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (2017) + EU member state DPIA whitelists and blacklists (2019)
- French DPA/CNIL -- Privacy Impact Assessment resources *(available in French and English),* including guidance, templates, knowledge bases, IoT examples, infographic, and a free software tool (2018)
- Spanish DPA/AEPD's modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) dirigido a Administraciones Públicas (2019) *(available in Spanish)*
- Australian OAIC -- Public Sector Chief Information Officer Council (PSCIOC) Guide to undertaking privacy impact assessments
- New Zealand Privacy Commissioner -- Privacy Impact Assessment Handbook
- Canadian OPC -- PIAs guidance
- Bureau of Justice Assistance -- U.S. Department of Justice, Guide to Conducting Privacy Impact Assessments: for State, Local, and Tribal Justice Entities (2012)
- NIST Privacy Framework A Tool for Improving Privacy through Enterprise Risk Management
- Sidewalk Labs, Responsible Data Use Assessment - Digital Innovation Appendix Section 2.2.3, page 237 - 295
- UN Global Pulse, Risks, Harms, and Benefits Assessment
- SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond

Acknowledgements / 謝辞

Co-leads / 執筆者代表

Kelsey Finch, Senior Counsel, Future of Privacy Forum

Michael Mattmiller, Director of Government Affairs, Microsoft

Task Force Members: / 参加メンバー

Pasquale Annicchino, Lex Digital and Archimede Solutions

Sean Audain, Wellington City Council

Chandra Bhushan, Quantela

Dylan Gilbert, Privacy Policy Advisor, NIST

Naomi Lefkovitz, Program Manager, NIST

Jacqueline Lu, Co-Founder, Helpful Places

Eugene Kim, Associate Director, Privacy and Data Governance, Sidewalk Labs

Dan Wu, Immuta

Contributors and reviewers: / 貢献者および批評者

Hector Dominguez-Aguirre, City of Portland

Dilip Krishnaswamy, VP of New Tech R&D, Reliance Jio

Masaru Yarime, Ph.D., Associate Professor, Division of Public Policy (PPOL), Hong Kong University of Science and Technology

About the G20 Global Smart Cities Alliance

2019 年 6 月に設立された「G20 Global Smart Cities Alliance for Technology Governance」は、スマートシティテクノロジーの責任ある倫理的な利用のための共通原則を、自治体・政府、民間企業、市民の連携を目指すものです。官民協力の国際機関である世界経済フォーラムがアライアンスの事務局を務めます。

本アライアンスでは、政府、民間企業、市民社会のグローバルな専門家が、倫理的なスマートシティの実現に必要なモデルポリシーを策定するために、世界中の政策をまとめ、分析しています。

アライアンスのモデルポリシーやその詳細については、こちらをご覧ください。
https://globalsmartcitiesalliance.org/

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Cover: Forum Stock Images

Model Policy

Privacy Impact Assessment

G20 Global Smart Cities Alliance

This policy is considered foundational to the G20 Global Smart Cities Alliance policy roadmap's principles of **privacy & transparency.** You can find supplementary content on our website[1] to provide practical support for adopting and implementing this policy.

Background

Cities around the globe are growing at an incredible rate, with residents flocking to the economic opportunities and amenities that they provide. City governments are responding to their continued growth in part by deploying technologies and "smart city" solutions that enable more citizen-centred services and progress to more sustainable, inclusive, and open cities. In order to achieve these goals, cities and communities of all sizes must ensure that

[1] Visit https://globalsmartcitiesalliance.org/

data generated by these technologies about individuals and their communities is appropriately protected and secured.

The collection of data occurs in every day city operations, from paying a utility bill, to browsing a web page, and increasingly walking down a city street, riding public transit, or driving on a city-maintained road. The use of smart city technologies -- such as sensors, connected devices, and always-on data flows that manage transportation systems, support real-time infrastructure maintenance, automatically administer public services, enable transparent governance and open data, and support emergency services in public areas -- can provide real benefits to governments and communities. While well-intentioned, they can also create the risk of individual privacy harms and raise fears of surveillance that negate the benefits of city life and actively discourage individuals from engaging with public spaces.

The increasing changes and complexity of emerging technologies, business systems, laws and regulations, as well as increased public scrutiny, require cities to take appropriate steps to proactively and methodically embed privacy and data protection into their activities. While privacy is traditionally understood as a wider concept encompassing different rights, data protection involves the protection of the individual in relation to the collection, use, and processing of personal data.

Cities must balance their own need to use and share data to conduct business with the broader public welfare and individual privacy interests in a way that builds and maintains public trust. Without public trust, the benefits of smart city technologies will be ultimately unsustainable. Cities must invest in policies and practices that will help individuals, local communities, and technology providers maximize the benefits of responsible data use while minimizing privacy risks to individuals and communities.

By implementing Privacy Impact Assessment (PIA) policies, cities can establish a consistent method for identifying, evaluating, and addressing privacy risks. Drafting a model PIA policy is a complicated process, as wide variation exists in cultural and legal approaches to privacy and data protection around the world. In this policy, we hope that by prescribing the process that should be followed and the issues that must be considered, we increase the likelihood that cities will more confidently consider and address privacy risks in a manner consistent with community expectations.

Contents

Model Policy

Objectives

A City must work to find a fair balance between gathering information to provide needed services and protecting the public's privacy, especially when deploying innovative smart city technologies. Privacy Impact Assessments (PIAs) are essential privacy assessment tools. PIAs consist of a set of processes to identify and manage privacy risks throughout the complete data lifecycle, from collection through disposal. Conducting a PIA prior to the acquisition or use of technologies in a smart city can increase transparency and accountability; support public trust; mitigate potential privacy harms or disparate impacts before they occur; improve compliance and reduce legal risk; and enable more confident and consistent decision-making about data and technology by city officials, their partners, and the public.

A City's PIA Policy should identify issues to be addressed and processes to be followed in the identification and mitigation of privacy risks. Specifically, a PIA Policy should:

- Articulate specific purposes for data and technologies as well as potential privacy risks and mitigation measures, and assess them against the City's and community members' values, priorities, and legal rights.
- Be integrated throughout the full project and data lifecycle (including intersections with the City's obligations around procurement, data security, accessibility, and public records).
- Address all data collected by a technology or service, not just data considered "personal" or "personally identifiable" at a particular moment in time.
- Facilitate communication and cooperation about privacy practices internally and externally, and create a clear understanding about when the City should reconsider a particular technology or notify its communities, partners, and technology providers.
- Encourage innovation by supporting ethical decision-making and optimizing beneficial uses of data while minimizing adverse consequences to individual privacy and society as a whole.
- [More participatory option]: Incorporate meaningful and inclusive opportunities for public engagement and decision-making about data and technology practices.

Examples:

- http://www.longbeach.gov/globalassets/health/healthy-living/office-of-equity/clb_toolkitbook_singlepages
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Foundations for Privacy Impact Assessments

Foundational procedural components to support the specific goals of the PIA policy, and its overall objective of maximizing societal benefits and minimizing risks to individuals and communities.

1. Organizational Values and Risk

a. Cities should explicitly identify the public values, priorities, and privacy principles against which particular technologies or services will be assessed during the PIA process.

Examples:

- NYC's IOT Guidelines
- Seattle's Privacy Principles
- Barcelona's Digital Service Standards
- India's DataSmart Cities Strategy

b. Cities should explicitly identify the legal standards and authority, as well as existing City policies and principles, against which particular technologies or services will be assessed during the PIA process.

c. PIAs should take into account considerations beyond legal compliance when assessing risks and benefits, including ethics, equity, and public engagement. These considerations should include not just impact on individuals but also groups.

d. [Higher maturity option]: The PIA process may include a rough preliminary scoring of opportunities based on values identified above.

Examples:

- https://wellington.govt.nz/~/media/about-wellington/emergency-management/files/covid-19/wcc-privacy-impact-assessment-digital-contact-tracing.pdf?la=en

e. [More participatory option]: Engage city staff and the public, especially vulnerable populations, to determine these broader public values, principles, and risk thresholds. Models include citizens' councils, citizens steward program, citizens' assemblies, digital models to upvote or budget city finances, public annotation of drafts, and/or social media engagement.

2. Scope and Timing

a. An Initial Assessment (or other threshold analysis to determine whether a full PIA is required) should be conducted:

i. As early as possible in the development or procurement of any new technology [and privacy-conscious protections built into the procurement criteria or development path for a technology]. Retrofitting a system to reduce privacy risks after it is designed or implemented has proven to be expensive.

ii. When planning material changes to existing processes and systems, including project updates that may include new data activity or changes in scope.

b. A full or an updated PIA should be conducted when required by regulation or City policy or when the Initial Assessment indicates that:

i. New technologies, new purposes, or new processes for data that may personally identify individuals are to be introduced.

ii. Significant changes to policies, business processes or systems are planned that may affect the physical or logical separation of personal information from other information within a system.

iii. Sensitive data is to be processed, or the technology or service may enable high-risk data processing [(such as scoring/profiling individuals, systematic monitoring, large scale processing, merging or matching data from multiple sources, targeting of children or vulnerable individuals, risk of physical harm, or the use of new technologies or the novel application of existing technologies)].

iv. When the technology or system enables automated or assisted decision making that may have legal or similarly significant effects on individuals.

c. When required, a PIA should be conducted before the acquisition or deployment of a data collecting technology into the city's environment or into the decision-making processes of a local government.

d. PIAs should be used to evaluate all data collected by a technology or service, not just data considered legally "personal" or "personally identifiable" at the time it is collected.

e. A PIA should be only one part of a comprehensive privacy program. It should sit alongside methods such as non-collection of data, privacy skills training, regulation, and auditing and publishing of PIAs within each local government or authorities' methods.

3. Tools and Components

a. Cities should develop and conduct a preliminary Initial Assessment or other threshold analysis in order to reveal whether further review is required, such as the completion of a full PIA [or an ethical impact assessment for non-personal data].

b. Initial Assessments should contain a preliminary assessment of privacy risks engendered by the system, product, or service, and may include high-level data flow diagrams or preliminary data and use characteristics.

> **Examples:**
> - Helsinki Initial Assessment
> - Seattle's PIA Policies
> - Toronto's PIA Policies

c. If it is determined that a full PIA is required, it should comprise the following components (see "Fundamentals of a PIA" below):

i. An assessment of privacy risks - Conducting a privacy risk assessment helps an organization to identify privacy risks engendered by the system, product, or service and prioritize them to be able to make informed decisions about how to respond to the risks.

ii. A risk response determination - In determining how to respond to assessed risks, cities should refer to their organizational values and risk tolerance determination. Response approaches include:

- **mitigation** (risks are mitigated to an acceptable level of residual risk through technical and policy measures such as data minimization),
- **transfer/sharing** (risks are shared with other parties such as through contracts or insurance; consent mechanisms are a form of risk sharing with individuals. Individuals should be able to reasonably understand the relevant risks before being asked to provide consent),
- **avoidance** (cities may choose not to use certain technologies or conduct certain types of data processing where the risks outweigh the benefits, or
- **acceptance** (cities may choose to accept the risk where the likelihood or impact of adverse consequences are low, and the benefits are great).

iii. Requirements and selected controls that enable the City to

- **meet applicable legal obligations** (organizational-level privacy requirements are a means of expressing the legal obligations, privacy values, and policies to which a city intends to adhere. Organizational-level privacy requirements may be derived from a variety of sources,

including legal environment (e.g., laws, regulations, policies or cultural values; relevant standards; and privacy principles) and

- **address the risks** determined to be mitigated.

d. Cities should consult local data protection authorities and other privacy and data protection experts for specialized guidance, templates, and tools for conducting PIAs and assessing privacy risk (See Additional Guidance below)

> A proven method in conducting a PIA is the workshop method, which starts with an initial meeting, to which all necessary stakeholders are invited. The assignment of responsibilities takes place at the initial meeting. At the impact assessment workshop (or workshops) after the initial meeting the experts have in advance sorted out aspects connected to their responsibilities, whereas the documentation of the data into the tool can be made jointly.

4. Roles and Responsibilities

a. A designated senior official, such as a Chief/City Privacy Officer (CPO) [with the support of a dedicated privacy team] should be responsible for:

i. Developing appropriate templates, resources, and components for the City's Initial Assessment and PIA tools,

ii. Setting the standards and qualifications of the resources permitted to conduct a PIA,

iii. Reviewing Initial Assessment or otherwise determining where a PIA is necessary (including re-review of existing PIAs),

iv. Conducting and approving of PIAs, including providing requirements and recommendations to mitigate privacy impacts.

v. Liaising with other officials to resolve privacy and security concerns raised during the course of the PIA, and

vi. Determine the City's response to identified privacy risks.

b. Agency/department/programmatic officials should be responsible for:

i. Providing appropriate information and documentation about the proposed technology and its use (e.g., technology functionality, business case, proposed purposes, costs for ongoing privacy and security protections, etc.),

ii. Completing Initial Assessment and assisting in the completion of a full PIA, where appropriate,

iii. Implementing the data use and management plan and all appropriate safeguards identified in the PIA as necessary to mitigate risks associated with the proposed technology,

iv. Ensure that the PIA policy is communicated to staff, and that staff are given sufficient time and resources to participate in the PIA process, and

v. Authorize and approve PIAs, as appropriate, prior to the implementation of privacy-impacting technologies.

c. An executive or senior official, such as a City Manager or Chief Technology Officer, should have authority to oversee compliance with the PIA Policy, including:

i. Ensuring the PIA Policy is communicated to all staff, implemented, and enforced,

ii. Ensure information is shared and accessible to the greatest extent possible, while respecting privacy and security requirements,

iii. Provide appropriate budget and organizational structure to enable the designated senior official for privacy and other staff to routinely conduct PIAs,

iv. Develop and implement appropriate accountability measures (e.g., escalation procedures, staff training and awareness, reporting systems and intake for complaints or potential threats related to privacy),

v. Monitor the effectiveness and outcomes of the PIA policy, and

vi. Review alignment of PIA schedules with Smart City project schedules.

d. Additional City officials and external stakeholders should be consulted where appropriate given the nature of the particular technology or service, such as:

i. An executive representative to advise the PIA program and champion department participation,

ii. CISO or other IT experts to assist in design of technology systems and assessment and mitigation of data security risks,

iii. City attorneys or legal counsel to ensure compliance with legal standards, including applicable data protection regulations,

iv. Public records officers and open data officials to identify circumstances in which data might be disclosed (intentionally or by law),

v. Procurement officials,

vi. Officials from other City agencies to identify additional interests in the data or technology,

vii. External subject matter experts,

viii. Technology partners, and

ix. Members of impacted communities.

e. [More mature option]: A senior privacy officer is supported by specialized data protection, risk management, and security professionals who are experts in conducting PIAs. The data privacy team is supported by a citywide network of "privacy champions," who are subject matter experts within particular departments able to assist in the PIA process. The PIA team is able to build institutional knowledge and best practices, support more consistent privacy decision-making across the City, and identify opportunities to improve PIA processes and outcomes.

Examples:
- Toronto RMIS w/in I&T division
- Seattle privacy champions

f. [More participatory option]: An external body or organization is engaged to provide input, make recommendations, utilize community expertise, or provide approval to PIAs. The group includes diverse stakeholder representatives, including privacy and data protection experts and members of the community.

Examples:
- Seattle Surveillance Working Group
- Oakland Privacy Advisory Commission

5. Monitoring and Recordkeeping

a. All Initial Assessments and PIAs should be thoroughly documented in writing, and be maintained in accordance with the City's record retention schedule. Examples: Helsinki Data Register, Seattle PIA Reviews

b. Any technologies determined to be exempt from PIA review should also be logged and documented in writing.

c. PIAs may be classified and categorized if there are multiple PIAs for a city.

d. Local Governments should create a secondary, aggregated PIA process, performed [three yearly] to assess the way systems and data interact to prevent data that was once considered non-personal from, over time, become identifiable; by evaluating all data generated by an IOT technology or service together, cities can future-proof their assessments to a greater degree.

e. A designated senior official for privacy should review the PIA policy annually (or sooner if necessary), and update it as necessary.

f. City departments, divisions, or programs and any partners or service providers should assess their own degree of compliance with the PIA Policy, [such as by conducting internal audits, program reviews, or program evaluations].

g. In the event that the City receives a privacy complaint or experiences a privacy breach, a designated senior official for privacy should investigate and make recommendations, as necessary, to remedy the situation.

h. [Higher maturity option]: Cities should develop and maintain an inventory of systems/products/services that process data, including the roles of owners or operations with respect to the systems and their components; the data provenance; the data actions of the inventoried systems; the purpose(s) for the data actions and the data processing environment.

Precedents:

- Seattle's inventory of surveillance tech
- Amsterdam's IoT Registry
- Barcelona's Sentilo
- City of Boston's pilot of Digital Transparency in the Public Realm
- NIST privacy framework

6. Transparency & Engagement

a. To the extent possible, Cities should make all PIAs available to the public on an easily accessible, outward-facing website.

> **Precedents:**
> - Seattle PIA and SIR inventory
> - Wellington DCTT PIA

b. Cities should develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

c. Cities should develop additional mechanisms (e.g., notices, internal or public reports) to communicate data processing purposes, practices, and privacy risks associated with smart city technologies, informed by relevant PIAs.

d. [More participatory option]: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.

> **Supplementary guidance:**
> - PIAs should avoid using acronyms, slang, or other terms which will not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.
> - Signage should be provided in-situ as needed to comply with relevant local privacy regulations [and should be considered for novel or new deployments of IoT technologies more broadly in order to inform the public of data collection and processing activities].

Fundamentals of a Privacy Impact Assessment

This section describes the fundamental issues or questions that a PIA should address, in order to enable cities and their partners to effectively identify and mitigate potential privacy risks while maximizing the public benefits of data and technology.

A PIA should clearly and understandably:

1. Identify the City departments, divisions, or programmes and any partners or service providers who will use or be accountable for the technology.

2. Describe the technology to be designed or acquired and a description of its general capabilities, functionality, the type of data that it is reasonably likely to generate, and the sources and accuracy of any personal information collected, including reasonably foreseeable surveillance capabilities outside of the City department's proposed use.

3. Describe the purpose and proposed use of the technology, including its intended value and benefit to individuals, the community, and society at large [and any data or research demonstrating those benefits]. Describe the problem the technology seeks to solve, and whether any less invasive alternatives exist.

4. Describe the City's authority to collect, use, and disclose personal data relevant to the proposed technology, as appropriate.

5. Describe any public values, principles, legal standards, and organizational risk frameworks against which the technology is being assessed.

6. Assess and describe the potential privacy risks associated with the proposed use of the technology, [including the likelihood of such risks occurring and the severity of the potential impact on individuals and communities.]

7. Describe the City's risk response to the identified risks, given organizational values and risk tolerance (e.g., mitigation of risks, transfer/sharing of risks, avoidance of risks, or acceptance of risks).

8. Describe a clear use and data management policy for the proposed use of the technology, including:

    a. How and when the technology will be deployed or used and by whom (including, as appropriate, descriptions of who has ownership or licensing rights to the data under what conditions).

    b. Any additional rules that will govern the technology (including legal standards that must be met before the technology is used, such as for the purposes of a criminal investigation).

    c. How data will be securely stored and destroyed or de-identified.

    d. How long data will be retained in identifiable and non-identifiable forms.

e. How access to data will be monitored and controlled, [including access logs and audits].

f. Whether the technology or data will be shared, and if so under what conditions (including both routine sharing, such as with partners or service providers, other government entities, researchers, public records requests, or open data, and in exigent circumstances).

g. What training and accountability measures will help ensure that all personnel who operate the technology or access data use it only in compliance with City policy.

h. What safeguards are in place to ensure the confidentiality, integrity, and availability of data (including protection from threats like ransomware, malware, or IoT vulnerabilities).

i. Any other legal, organizational, physical, and technical safeguards intended to mitigate potential privacy risks associated with use of the technology.

9. Describe any community engagement held and any future community engagement plans, any comments received and City responses given, and City conclusions about potential neighbourhood and disparate impacts that may result from the acquisition and use of the technology.

10. Describe any emergency or civil defence legislation that may change the way the data is used or the processes governing it.

11. Describe how the potential impacts of the technology on civil rights and liberties and potential disparate impacts on marginalized communities have been taken into account and mitigated.

12. Describe the availability of funding for ongoing privacy and data protection costs related to operation of the technology (such as personnel, legal compliance, auditing, data retention, and security costs).

Additional Guidance & Resources

Examples of City PIAs

- Helsinki Data Register and DPIA tools
- Huron County Privacy Impact Assessment Policy
- Santa Clara County Surveillance Use Policies
- Seattle PIA Reviews and Surveillance Reports
- Toronto Privacy Impact Policy
- Wellington Digital Contact Tracing PIA

Guidance on conducting a PIA or DPIA

- The former Article 29 Working Party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (2017) + EU member state DPIA whitelists and blacklists (2019)
- French DPA/CNIL -- Privacy Impact Assessment resources *(available in French and English),* including guidance, templates, knowledge bases, IoT examples, infographic, and a free software tool (2018)
- Spanish DPA/AEPD's modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) dirigido a Administraciones Públicas (2019) *(available in Spanish)*
- Australian OAIC -- Public Sector Chief Information Officer Council (PSCIOC) Guide to undertaking privacy impact assessments
- New Zealand Privacy Commissioner -- Privacy Impact Assessment Handbook
- Canadian OPC -- PIAs guidance
- Bureau of Justice Assistance -- U.S. Department of Justice, Guide to Conducting Privacy Impact Assessments: for State, Local, and Tribal Justice Entities (2012)
- NIST Privacy Framework A Tool for Improving Privacy through Enterprise Risk Management
- Sidewalk Labs, Responsible Data Use Assessment - Digital Innovation Appendix Section 2.2.3, page 237 - 295
- UN Global Pulse, Risks, Harms, and Benefits Assessment
- SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond

Acknowledgements

Co-leads

Kelsey Finch, Senior Counsel, Future of Privacy Forum

Michael Mattmiller, Director of Government Affairs, Microsoft

Task Force Members:

Pasquale Annicchino, Lex Digital and Archimede Solutions

Sean Audain, Wellington City Council

Chandra Bhushan, Quantela

Dylan Gilbert, Privacy Policy Advisor, NIST

Naomi Lefkovitz, Program Manager, NIST

Jacqueline Lu, Co-Founder, Helpful Places

Eugene Kim, Associate Director, Privacy and Data Governance, Sidewalk Labs

Dan Wu, Immuta

Contributors and reviewers:

Hector Dominguez-Aguirre, City of Portland

Dilip Krishnaswamy, VP of New Tech R&D, Reliance Jio

Masaru Yarime, Ph.D., Associate Professor, Division of Public Policy (PPOL), Hong Kong University of Science and Technology

About the G20 Global Smart Cities Alliance

Established in June 2019, the G20 Global Smart Cities Alliance on Technology Governance unites municipal, regional and national governments, private-sector partners and cities' residents around a shared set of principles for the responsible and ethical use of smart city technologies. The World Economic Forum, the International Organization for Public-Private Cooperation, serves as secretariat for the Alliance.

Through the Alliance, global experts from government, private-sector partners and civil society, are compiling and analysing policies from around the world to identify model policies necessary for successful, ethical smart cities.

You can find more model policies and more details about the Alliance at:
https://globalsmartcitiesalliance.org/

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Cover: Forum Stock Images