



Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*

- Such as:**
- A social media or search company gathering, or sharing, user data without the consent of those users
 - Information and communication service providers operating in or expanding into new markets, which agree to share information about political activists or members of persecuted communities with governments that use it to violate those people's rights
 - Data brokers selling comprehensive consumer profiles as a raw product without the consent of those individuals
 - The digital transformation of various industries through the Internet of Things (IoT), including home appliances, car manufacturers, toy companies and many others, leading to a ubiquitous processing of personal information with a lack of human oversight, creating potential impacts on privacy where this data is used and shared.



HIGHER-RISK SECTORS:

- **Multiple Segments of the Technology Industry:**
 - Telecommunications, Internet Service Providers, and Web Hosting companies
 - Data Center or Cloud Service providers
 - Social Media platforms, and search engine, email and messaging service providers
 - Providers of web or mobile phone Apps
 - Companies supporting online communities and gaming
 - Consumer tech devices and service providers
 - IT firms providing digital services to government agencies
 - AI development companies (developing AI solutions that process or require handling of customer data)
- **Non-technology companies** whose business model is increasingly tied to the use of data on customer habits or movements, such as household appliance manufacturers and automotive companies. Increased digitalization across industries, the use of IoT and AI etc., also increases the types and number of companies collecting and processing personal data.
- **Data brokers** that collect data (e.g. from the internet, government sources etc.) and buy it from other companies (e.g. credit card companies) to either sell comprehensive consumer profiles as a raw product or sell big data analytics as a service (e.g. for risk evaluations, price optimization, targeted advertising).



KEY QUESTIONS FOR LEADERS TO ASK OR BE ASKED:

- How do we know we have a clear understanding, across our operations, of the data we collect and hold?
 - How central to our core product or service offering is the collection and retention of this information?
 - How have we involved human rights expertise to understand potential impacts on those people whose personal data we source, use or provide to others, particularly vulnerable or marginalized people?

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*

RED FLAG NO.



16

RED FLAGS IN THE VALUE CHAIN



KEY QUESTIONS FOR LEADERS TO ASK OR BE ASKED:

- Do the incentives that drive our data collection undermine the ability of people to decide whether to give their consent to us collecting and using it?
- How confident are we that the entities we are selling to, or sharing data with, will not expose, misuse or abuse that data?
- Have we built in sufficient privacy protections and other mitigations against intentional or unintentional misuse when collecting, handling and sharing personal data?
- How adequate are our scenario planning, training and action plans for potential breaches of data security?

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



RISKS TO PEOPLE

There are a range of reasons why companies in diverse sectors are collecting and holding data. For example, private hospitals and pharmaceutical companies may do so to improve diagnoses, improve treatment plans and develop medicines; banks may use personal and transaction data to identify fraud; and autonomous vehicle companies may seek to monetize data about customer driving habits to enable individuals to improve insurance premiums. Even so, **in order to fully realize these benefits for businesses and people, risks to people must be managed.** This is particularly true in the context of companies whose business models rely on collecting, holding or monetizing data about customers and users.

- **Right to Privacy:** In the digital age, privacy risks linked to data breaches for companies that are collecting or holding consumer information are increasingly prevalent, and appropriate operational actions must be taken to manage the risks that such breaches pose for consumer privacy. However, as a company's business model becomes increasingly reliant on the collecting, holding or sale of consumer data, there are inherent and pervasive privacy risks that need to be addressed and managed at a more strategic level. Examples of the types of companies that have such business models include:
 - **Data brokers** that build and sell detailed personal profiles by aggregating information from public records, online activity, purchases, and other sources — often without individuals' knowledge or direct consent. People have little control or transparency over what data is collected, how it's used, or who it's sold to, and such profiles can be used in ways

that affect access to employment, credit, insurance or even enable fraud.

- **Search engine advertising systems** that match paid advertisements to users' search queries, converting expressions of curiosity, need, or interest into commercial signals that generate revenue for the company while sharing users' personal data with third parties without consent.
- **Social media and video streaming platforms** are increasingly making continuous monitoring and user data monetization a structural feature of their business models, by engaging in extensive user surveillance to generate ad revenue, indefinite data retention, and sharing information broadly. These activities create significant privacy risks, including through cross-platform tracking, profiling of sensitive personal attributes, data-sharing with third parties, and limited user control over collected information. A [2024 report by the US Federal Trade Commission](#) found that *"the business models of many of the companies incentivized mass collection of user data to monetize, especially through targeted advertising, which accounts for most of their revenue."* (see also Red Flag 6).
- **Freedom from Arbitrary Attacks on Reputation and Right to an Adequate Standard of Living:** Where personal data becomes accessible to the public, this data can be used to threaten individuals or tarnish their reputations, which can in turn impact victims' mental health, job prospects and livelihoods.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



RISKS TO PEOPLE

- **Government Requests Leading to Abuses of Freedom of Expression and other Human Rights:** For example, where governments demand the company hands over:
 - Personal information regarding individuals belonging to politically or ethnically persecuted groups, which compromises the safety, security and freedom of impacted individuals.
 - The communications history of political activists or human rights defenders and use it to identify, intimidate, threaten, detain and even torture them.
 - Data about social media and other online activities of LGBTQI people that is used to violate their right to non-discrimination and rights to liberty and security.
- **Risks to the Right to Non-Discrimination:** Where data are used, shared or sold to third parties who use them in algorithmic decision-making that impacts their access to credit, welfare services, insurance or other services. (See Red Flag 5).
- **Ubiquitous processing of personal data:** Increased digitalization and use of IoT, AI, facial recognition and other digital solutions, lead to a substantial increase in the creation and use of personal data, which increases the risk of that data being misused. [A recent study](#) of smart home apps shows that devices collect extensive user data, often without clear disclosure, and a sizable portion is tied to tracking or user identification. Some of the apps also share such information with third parties and data brokers, without the clear consent of the individuals to whom the data belongs.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



RISKS TO THE BUSINESS

- **Regulatory Risks and Fines:** Failure to protect user or customer privacy can lead to investigations, scrutiny and sanction, and [many jurisdictions around the world](#) are debating and enacting stricter laws to govern privacy, affecting multinational companies domiciled all over the world. The most notable of these are the EU's General Data Protection Regulation which governs how personal data must be collected, processes and erased, [and sets two-levels of fines](#). Further, for companies whose business models are structured around data collection, use and monetization, regulatory risks and fines are increasingly prominent. For example:
 - The business models of generative AI tools rely on continuously training and refining large language models using vast quantities of data scraped or sourced at scale, including personal data. This model can create structural risks to privacy and data protection rights, particularly where individuals are unaware their data is being processed or lack any meaningful ability to consent, object, or seek remedy. In 2024 Italy's data regulator fined **ChatGPT/OpenAI** for processing personal data without adequate legal basis and with insufficient transparency about how personal data were used for training. This resulted in a €15 million administrative fine and a required corrective action plan.
 - Digital platforms whose business models prioritise rapid user growth and engagement often rely on default settings that maximise visibility, interaction, and data flows, including for child users. These design choices can structurally undermine children's rights to privacy and protection, particularly where

safeguards require active user intervention rather than being enabled by default. In 2023, [TikTok was fined €345 million](#) for default public settings allowing the viewing of children's profiles and messaging without consent, exposing minors to privacy risks and potential exploitation (see also Red Flag 8).

Other examples of regulatory action are as follows:

- In 2024, vulnerability in Facebook's "View As" feature allowed hackers to access user tokens and personal data for 29 million accounts globally. Hackers could misuse names, contact info, location, and other sensitive data. [Regulators fined Meta €251 million](#) for failing to protect users against this exposure.
- In 2024, [Clearview was fined €35.5 million](#) for scraping billions of images from the web to build a facial recognition database used by law enforcement, without user consent.
- In 2021, [WhatsApp was fined €225 million](#) for forcing users to accept updated terms, effectively imposing a "consent-or-lose-access" model. Coerced processing of personal data violated transparency and fairness principles.

In the United States, individual states have also put in place privacy regulations that apply to all industries. One such example is [California's Consumer Privacy Act](#).

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



RISKS TO THE BUSINESS

- **Legal Risk and Financial Settlements or Penalties:** An increasing number of companies have been subject to lawsuits over inadequate action to address risks to people throughout the data lifecycle, and even prosecution. Examples include the following:
 - In October 2025, Myanmar civil society groups [sued Norwegian telecom firm Telenor](#), alleging it passed sensitive customer data to Myanmar's military junta after the 2021 coup, which was then used to track and target activists and civilians, enabling arrests, torture, and potentially even executions.
 - In May 2025, [Google agreed to pay \\$1.375 billion](#) to resolve a lawsuit in which the company was accused of unlawfully collecting sensitive personal data – including users' geolocation information, biometric face and voice identifiers, and incognito browsing activity – without adequate consent.
 - **Equifax**, the US consumer credit score company, [paid \\$425 million following a data breach affecting 147 million people in 2017](#), some of whom suffered identify theft, fraud and related legal or other costs.
 - In 2023, the [US Federal Trade Commission \(FTC\) charged Amazon-owned home security company Ring](#) with violating users' privacy by handling and storing consumer data without restrictions or consent and by failing to implement basic security measures. The FTC required **Ring** to delete improperly accessed data, enhance security programs, and pay roughly \$5.8 million in refunds to affected customers.

In 2021, [users of Amazon's Alexa devices brought a lawsuit against Amazon](#) arguing that the company's Alexa voice assistant deceptively recorded and retained users' private conversations without adequately disclosing how the data would be stored or used, undermining users' reasonable expectations of privacy. In 2025, a [U.S. federal judge in Seattle ruled](#) that the plaintiffs met the legal threshold to sue in a nationwide class action, which will allow the plaintiffs to pursue large-scale claims against **Amazon** as a group, rather than filing individual claims. In Illinois, also in 2025, another [federal judge certified a class of roughly 1.2 million users](#) of **Amazon's** Alexa in a class action lawsuit alleging the company unlawfully collected their voice data. At the time of publication, both lawsuits are ongoing.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



RISKS TO THE BUSINESS

- **Reputational Risk.**
 - **Loss of Trust:** In the US, **Meta** faced [significant public and political backlash](#) after introducing a new Instagram feature that lets users share real-time location data on a map, with lawmakers from both major U.S. parties urging the company to roll it back due to child safety and privacy concerns. Confusing controls and reports of location data being exposed without clear consent damaged user trust in the feature, in addition to further exposing **Meta** to regulatory pressure and reputational harm.
- **Stock Price Risk:** There have been a number of reports about the impact of high-profile data breaches and sharing of sensitive user data with third parties on company stock prices.
 - In 2025, following disclosure of a customer data breach affecting 23 million users, shares of the Korean communication service provider [SK Telecom](#) dropped up to 8.5%.
 - The **Facebook** and [Cambridge Analytica scandal](#) of 2018 [reportedly led to a \\$119 billion dollar loss in market value.](#)

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



WHAT THE UN GUIDING PRINCIPLES SAY:

**For an explanation of how companies can be involved in human rights impacts, and their related responsibilities, see [here](#).*

- **A company can cause** an adverse impact on the right to privacy of any stakeholder group that it collects data on, and at any stage of the data lifecycle.
 - **When Collecting Data:** Although there are arguments that businesses obtain a “conscious compromise” from users about the exchange of information for goods and services, they may cause an impact on the right to privacy if the customer is not “truly aware of what data they are sharing, how and with whom, and to what use they will be put.” (The Right to Privacy in the Digital Age. OHCHR, A/ HRC/27/37).
 - **When Holding Data:** A company may not have in place adequate security protections such that a human or system error results in personal data being accessible by third parties.
- A company's use or mismanagement of data may **contribute** to a range of human rights harms depending on the context.
 - Where a company suffers a data breach and personal data is accessed by a third party who then uses it to threaten the individuals whose data was leaked.
 - Where a company makes a decision – even if consistent with local law - to provide personal data to a third party where it should have known that the data were likely to be used to abuse the rights of the data subjects concerned.
- Where companies (for example, banks and IT services firms, or automotive and insurance companies) work together to collect, analyze and interpret data in ways that lead to discriminatory pricing.
- Where a company sells or in some way shares personal data with business customers who in turn use those data in harmful ways.
- Where a company deploys AI solutions that gather user personal data in a non-transparent way, and without user consent (see also Red Flag 5).
- A company can be **linked** to a human rights harm where it has sold or provided data to a business entity or government, and that entity uses those data in ways that are unforeseeable but nevertheless lead to adverse impacts on people.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



POSSIBLE CONTRIBUTIONS TO THE SDGs:

Data about individuals can be used to advance **a number of SDGs** such as those listed below. Addressing impacts to people associated with this red flag can contribute to ensuring that this is done in ways that **do not simultaneously increase discrimination, or erode the privacy, reputation and well-being** of vulnerable communities.



SDG 10: Reduce inequality within and among countries.



SDG 9: Industries, innovation and infrastructure, in particular:

- **Target 9.5** Upgrading industrial sectors;
- **Target 9.b** Domestic technological development; and
- **Target 9.c:** Access to technology and the internet.



SDG 3: Healthy lives and well-being for all. Including by tackling disruptions to progress such as from the COVID-19 global pandemic.



SDG 5: Achieve gender equality and empower all women and girls, in particular:

- **Target 5.b** Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women



SDG 17: Strengthen the means of implementation and revitalize the global partnership for sustainable development, in particular:

- **Target 17.18** Increasing the availability of high-quality, timely and reliable data disaggregated to achieve development goals.

The [UN Secretary-General's Roadmap for Digital Cooperation](#) is an important resource to guide “all stakeholders to play a role in advancing a safer, more equitable digital world” even as technological solutions are used to achieve the SDGs. Additionally, the [UN Global Digital Compact](#), commits governments to upholding international law and human rights online and to taking concrete steps to make the digital space safe and secure.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN

DUE DILIGENCE LINES OF INQUIRY:

- Do we have policies, processes and practices that follow the principle of data minimization such that we only collect or purchase data to the degree that is absolutely necessary to accomplish specific tasks we have in mind?
- Have we conducted an assessment, and where necessary put in place mitigation plans, for privacy and other risks to people that may arise across the data life cycle including generation, collection, processing, storage, management, analysis and interpretation?
 - Have we done this for all stakeholder groups that may be at risk including employees, contract workers, prospective employees, customers and users?
 - Are we engaging expert groups and potentially affected groups to ensure we understand the risks they perceive or experience?
- Do we assess how our terms of service or policies for gathering and sharing customer data might increase human rights risks?
- Do we ensure that customers or users consent to how we gather and use their data, and that their consent is free and informed, including that they:
 - Know that we gather and are in control of data about them.
 - Are informed about how the data will be obtained and held, and for how long.
 - Understand the operations that will be carried out on their data.
 - Know how to withdraw their consent for the use of their data.
- Where we develop and/or deploy AI solutions that gather personal data, do we ensure that such solutions are built on sufficient transparency, user consent, human oversight and privacy protections?
- Where we buy data from another company, are we confident that it was legally acquired? Do we have ways to verify its accuracy?
- Where we sell or share data with third parties:
 - Do we understand how the third parties will use it and whether there are any risks of harm to particular populations?
 - Do we assess if they have the appropriate security and safeguards?
 - Do we have in place a data sharing agreement that follows best practice?
- Do we retain a clear and up-to-date understanding of “data journeys” such that we can, where needed, take meaningful steps to delete the data in the event that we find it is used for human rights abuses?
- If we transmit data from customer devices, or allow messaging between users, do we have in place end-to-end encryption to prevent third parties from decrypting conversations? Have we developed an approach that takes into account the human rights benefits that can come from allowing third parties to scan for content (such as the ability to support legitimate criminal investigations)?

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

RED FLAG NO.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN

DUE DILIGENCE LINES OF INQUIRY:

- If we face a risk of government demands for data where this may be used to abuse human rights, have we:
 - Assessed ourselves against the [Implementation Guidelines of the Global Network Initiative](#)?
 - Engaged with credible NGOs and human rights experts to understand these risks, and to prepare us to take action should government requests occur?
- Are our executives prepared for a breach?
- Do we have a comprehensive plan in place to respond to breaches, and specify how we'll handle informing stakeholders?
Are we clear on how we will provide for remedy if our actions contribute to the violation of user, customer, or employee privacy or other rights?

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



MITIGATION EXAMPLES:

**Mitigation examples are current or historical examples for reference, but do not offer insight into their relative maturity or effectiveness.*

- **Privacy Policy Hubs:** Several businesses are building “hubs” for their privacy policies. Hubs are a dedicated area where data subjects (visitors to a website, customers, users) can go to view: how their data is being used; where it’s being used; how their data is being collected and what type; terms of the policy; and where subjects can revoke consent. For example, **Disney’s [privacy hub](#)** also states how they protect children – their largest and most at-risk audience.
- **Cisco’s Trust and Transparency Center Online:** In 2015, **Cisco** launched the [Trust and Transparency Center online](#), which is dedicated to providing information, resources and answers to cybersecurity questions and to help manage security and privacy risk. The Centre includes **Cisco’s** Trust Principles, which describe their commitment to protect customer, product and company information, and it provides information about security policies and data protection programs.
- **Participation in the [Global Network Initiative](#):** **GNI** is a multi-stakeholder initiative comprising companies, civil society organizations, investors and academics. **GNI** provides a framework to help ICT companies respect privacy rights, integrate privacy policies and procedures into corporate culture and decision making and communicate privacy practices with users. Members commit to an independent assessment process about how **GNI** principles are integrated within their organization.
- **T-Mobile [Do Not Sell Links](#):** The California Consumer Privacy Act (2018) requires companies to post a clear and conspicuous link on their website that says, “Do Not Sell My Personal Information” through which consumers can opt out of the sale of their data to third parties. Some companies, like **T-Mobile**, apply this for all customers in the United States.
- **Using Leverage to Regulate Data Brokers:** In the United States, some business leaders (most [notably Apple CEO Tim Cook](#)) have called for a registry of data brokers to make their role in the collection, storing and selling of personal data more transparent and accountable.
- **The Microsoft Digital Crimes Unit:** [Microsoft’s digital crimes unit](#) exists to “fight against cybercrime to protect customers and promote trust in Microsoft.” It operates globally through the application of technology, forensics, civil actions, criminal referrals, and public/private partnerships and is staffed by “an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals located in 20 countries.”

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



MITIGATION EXAMPLES:

**Mitigation examples are current or historical examples for reference, but do not offer insight into their relative maturity or effectiveness.*

- **Privacy by design:** [Privacy by design is a proactive approach](#), adopted by many companies, that embeds privacy protections directly into the design and architecture of products and solutions, rather than reacting to privacy breaches, and aims to ensure that privacy is a default setting. Examples include end-to-end encryption of communications, storing user data on the user's device, rather than in the cloud etc.
- **Human Rights Impact Assessments:** Companies developing and deploying digital tools and solutions that process personal data can conduct human rights impact assessments at early stages of the development and deployment cycle, in order to identify and mitigate risks before they materialize. Examples include [Ericsson's 5G Human Rights Assessment](#), and the assessment of [Meta's expansion of end-to-end encryption](#).
- **Transparency reports:** Communication service providers are required by their license agreements to share information with law enforcement agencies under certain circumstances. While such requests typically need to be complied with under local law, communication service providers such as [Telenor](#) and [Telia](#) have established processes to evaluate government requests and deny access in cases where such requests are not aligned with legal requirements.

Additionally, the companies also publish annual government authority disclosure reports, in order to be transparent in terms of number and nature of requests received.

- **Push back on government requests:** Apps such as [WhatsApp](#) and [Signal](#) have threatened to leave markets such as India, Sweden and France, if forced to break encryption and share user data with the government. [Apple](#) also pushed back against government requests in India to remotely unlock and share data stored on user devices.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



ALTERNATIVE MODELS:

- **Consumer Products and Services:** A number of companies have launched privacy-oriented alternatives such as:
 - **Messaging App Signal:** One of the only apps that has its privacy-preserving technology always enabled and ensures there is never a risk of sharing moments or sending messages to a non-intended recipient. For more on messaging apps see [this article](#).
 - **Search Engine Swisscows:** [Swisscows](#) does not collect any of their visitors' personal information such as an IP address, browser information, or device information. They do not record or analyze search terms. The only data that Swisscows records is the total number of search requests it receives each day.
- **Enterprise Solutions:** A 2020 World Economic Briefing, [A New Paradigm for the Business of Data](#), (subsequently followed by briefings exploring similar themes in [2022](#) and [2023](#)), profiles a small number of enterprise and consumer solutions that prioritize privacy, user consent and data security. These include:
 - **Hewlett Packard Enterprise (HPE) and Continental:** HPE and Continental have created the Data Exchange Platform as a marketplace for mobility data. "It provides a secure, transparent, decentralized architecture for trusted vehicle sensor data sharing and payment, based on blockchain technology and smart contracts. It offers data sovereignty and includes a consent-management system for drivers."
 - **Inrupt:** "Instead of a company storing siloed snippets of personal data on their servers, users store it in interoperable online data stores giving them unprecedented choices over how their data is shared and used. They can, for example, share their fitness data with their health insurance company, or allow sharing between their thermostat and air conditioner. They can set time limits on sharing and change their choices at any time."
- **Designing generative AI tools with privacy in mind:** Several companies have introduced AI tools that are explicitly designed not to store or process personal data. These include:
 - **Proton Scribe:** [An AI writing assistance tool](#) built into the email service, that is only processed on the device, allowing neither Proton nor the AI to access other messages and ensuring that user data such as emails is never used to train the AI.
 - **Apple Whisper Notes:** Is a [voice-to-text transcription app](#), designed for offline, on-device transcription. The recordings never leave the device and are not logged or stored on any external servers.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



ALTERNATIVE MODELS:

- **Microsoft EdgeML:** Is a set of tools and models embedded within [Microsoft Edge](#) browser and other apps that perform AI/ machine learning tasks locally on the user's device. Examples include autofill suggestions, spell checking, voice recognition, and content personalization, all done without sending raw data to the cloud.
- **DuckDuckGo Duck.ai:** [Duck.ai](#) provides AI-generated summaries, answers, and search results, without logging user queries, IP addresses, or requiring a user profile. Additionally, the AI-generated answers are not based on user history and not used to train the AI model.



OTHER TOOLS AND RESOURCES:

- The Danish Institute for Human Rights, (2021) [Human rights impact assessment of digital activities](#)
- BSR (2025) [A Human Rights Assessment of the Generative AI Value Chain](#)
- Law Commission of Ontario and Ontario Human Rights Commission (2024) [Human Rights AI Impact Assessment](#)
- Ranking Digital Rights Investor Outlook (2021) [Investors need an updated digital rights playbook for 2021](#)
- Global Network Initiative resources:
 - [Implementation Guidelines](#)
 - [Public Assessment Reports on Independent Assessments of GNI Members](#)
 - [Country Legal Frameworks Resource](#): – Providing information on privacy protections in national legal frameworks
 - [2018/19 Report on Independent Assessments of GNI Members](#)
 - [Across the Stack Tool](#) – Aimed at providing an overview of roles and responsibilities of actors across the technology stack, in order to support due diligence efforts

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

RED FLAG NO.

Collecting, holding or monetizing data about customers or users in ways *that lead to adverse impacts on privacy, and other human rights.*



16

RED FLAGS IN THE VALUE CHAIN



OTHER TOOLS AND RESOURCES:

- [Human Rights and Big Data Project](#)
- Information is Beautiful, [Map of Data Breaches/Hacks](#): An interactive tool showing the world's largest data breaches and hacks since 2009 up until the present. The map includes examples from 15 industry sectors and multiple well-known corporations including.
- [UN Secretary-General's Roadmap for Digital Cooperation](#).
- [UN Global Digital Compact](#).
- UNDP (2025) [Human Development Report – A matter of choice: People and possibilities in the age of AI](#)
- [OHCHR B-Tech Project](#) (The B-Tech Project provides authoritative guidance and resources for implementing the United Nations Guiding Principles on Business and Human rights (UNGPs) in the technology space.)

This resource is part of Shift's collection of Business Model Red Flags, developed as part of the Valuing Respect Project and generously funded by Ministry of Foreign Affairs Finland, the Norwegian Ministry of Foreign Affairs, and Norges Bank Investment Management. Learn more at: shiftproject.org/valuing-respect