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
- Email or messaging service providers sharing information about political activists or members of persecuted communities with governments that then use that information to violate those people's rights
- Retailers, banks, airlines, hotels not adequately protecting the data they collect about customers such that those data are accessible to hackers and in some way become public
- Data brokers selling comprehensive consumer profiles as a raw product without the knowledge of those individuals

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 email and messaging service providers
  - Providers of web or mobile phone Apps
  - Supporting online communities and gaming
  - Consumer tech devices and service providers
  - IT firms providing digital services to government agencies
- **Non-technology companies that collect and hold personal data** e.g. health care, retail and financial services companies and then "non-technology" companies that use data on customer usage, habits or movements, such as household appliance manufacturers and automotive companies.
- **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:

- Have we established that the business benefit of collecting customer or user data actually outweighs the costs of protecting those data, and the risks of data breaches? Have we analyzed the relative merits of not collecting or holding this type of data?
- Do the incentives that drive our data collection undermine the ability of people 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?
- How adequate are our scenario planning, training and action plans for potential breaches of data security?

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

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, the following risks must be managed.**

- **Right to Privacy:** Where a company collects, holds or provides third parties with access to data about customers or users, there are inherent and widespread privacy risks. Examples include:
  - Where information about an individual is collected, sold or shared without their consent. This includes when data are used for purposes beyond those originally consented to by a "data subject."
  - Where data breaches result in individuals' personal financial or health data being publicly accessible.
  - Breaches of sensitive personal information, such as racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, sex, gender identity or sexual orientation, genetic data, biometric data, or data concerning health.

- **Freedom from Arbitrary Attacks on Reputation and Right to an Adequate Standard of Living:** Where the 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.

- **Government Requests Leading to Abuses of Freedom of Expression and other Human Rights:** For example, where governments demand the company hands over:
  - 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).

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

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.
  - In 2020, British Airways was fined €22 million when their website diverted users' traffic to a hacker website, impacting the data of over 400,000 customers.
  - In 2019 Marriot International was fined €110 million related to a cyber-attack through which personal data from over 339 million guest records were exposed.
  - In 2019, Google was fined €50 million due to a lack of meaningful consent about how data was being collected and used for the purposes of targeted advertising.
  - 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.

- **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. Examples include:
  - Facebook paying $550 million to settle a class action lawsuit from Illinois Facebook users accusing the company of violating an Illinois biometric privacy law.
  - An £18 billion class action claim against Easy Jet in which the data of 9 million customers was accessed by third parties in a cyber-attack
  - Equifax, the US consumer credit score company, paying $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.

- **Operational Costs Following Breaches:** Companies that experience a data breach faced immediate financial costs. The Home Depot breach of 56 million customer credit cards was estimated to cost $62 million to enable, among other steps: the post-breach investigation, call center staffing and monitoring of breached accounts for unusual activity. According to IBM's 2020 Cost of Data Breach report, the global average total cost of a data breach is $3.86 million.

- **Reputational Risk. Loss of Trust:** A 2017 Forbes article notes that according to a PwC survey, "only 25% of consumers believe companies handle their personal information responsibly and 87% will take their business to a competitor if they don't trust a company to handle their data responsibly." An International Data Corporation study found that "80% of consumers in developed nations will defect from a business because their personally identifiable information is impacted in a security breach."

- **Stock Price Risk:** There have been a number of reports about the impact of high-profile data breaches on company stock

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

RISKS TO THE BUSINESS

prices. The Facebook and Cambridge Analytica scandal of 2018 reportedly led to a $119 billion dollar loss in market value. A UK study notes that, "Companies that self-reported their security posture as superior and quickly responded to the breach event recovered their stock value after an average of 7 days. In contrast, companies that had a poor security posture at the time of the data breach and did not respond quickly to the incident experienced a stock price decline that on average lasted more than 90 days."

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

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.

- 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*.

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 3: Healthy Lives and Well-Being for all. Including by tackling disruptions to progress such as from the COVID-19 global pandemic.

SDG 5.B: Promote Empowerment of Women Through Technology

SDG 9: Industries, Innovation and Infrastructure, in particular
- 9.5: Upgrading industrial sectors;
- 9B: Domestic technological development; and
- 9C: Access to technology and the internet.

SDG 17.18: Partnerships
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.

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:

- 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 whether and 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 they can withdraw their consent for the use of their data.

- 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 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)?

- 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?

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:

- 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? Have we done scenario planning and trained all relevant teams about what to do in the event of data breaches? In particular, do we have a clear action plan to ensure we inform our customers or users of breaches as fast as possible?
- 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*.

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.
  - **Disney's** privacy hub also states how they protect children – their largest and most at-risk audience.
  - **Twitter's** privacy site includes information about how users' tweets, location, and personal information are used.
- **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."

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

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 that 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*, profiles a small number of Enterprise and consumer solutions that place privacy, user consent and data security at the core. 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."

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

OTHER TOOLS AND RESOURCES:

- Ranking Digital Rights Investor Outlook (2021) *Geopolitical risks are rising—and regulation is coming*.
- Institute for Human Rights and Business, *Data Brokers and Human Rights*.
- Global Network Initiative resources:
  - Implementation Guidelines.
  - 2018/19 Report on Independent Assessments of GNI Members.
- Harvard Data Science Review, Jeanette Wing, *The Data Life Cycle*.
- Human Rights and Big Data Project, *Developing an Online consent manifesto based on human rights*.
- 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.
- Data Guise, *Data Minimization in the GDPR: A Primer*.
- *UN Secretary-General's Roadmap for Digital Cooperation*.

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