



# Human Rights Assessment of the Software-as-a-Service Sector

May 2022



# Executive Summary

Software-as-a-service (SaaS) makes up the largest segment of the public cloud market.<sup>1</sup> SaaS services address numerous business needs, and they are behind many of the consumer-facing products and platforms we use every day. As these services become increasingly common, a deeper understanding of how SaaS services may impact human rights, and the appropriate actions to address those impacts, is needed.

To unpack the SaaS sector's connection to human rights, BSR worked with seven business-to-business (B2B) SaaS providers to conduct a sector-wide human rights assessment of the SaaS sector. This report identifies salient human rights risks and makes recommendations to SaaS providers on how to avoid, prevent, and mitigate adverse human rights impacts associated with their individual services and the sector as a whole.

## Connection to Downstream Impacts

In the context of the end-use of products and services, a B2B SaaS provider can impact human rights in two main ways: (1) through their own activities (e.g., misusing data or developing biased algorithms), or (2) through their customers' activities. For the latter, it is particularly challenging for SaaS providers to foresee the downstream human rights impacts that they may be connected to.

SaaS providers typically have low levels of visibility into the end-use of their services and the associated human rights impacts. However, due diligence related to end-use of products and services is increasingly expected from companies further up the value chain<sup>2</sup>, such as B2B SaaS service providers.

To address the downstream human rights impacts that they may be connected to, SaaS providers need to determine their company's connection to potential human rights harms. The actions that the company must take to avoid, prevent, and mitigate adverse human rights impacts depend, in part, on their attribution to such impacts.



## Differentiating Factors

Typically, when assessing the downstream impacts of a company's products and services, we focus on the end-user and the use case.<sup>3</sup> The most important considerations in evaluating the potential human rights impacts of SaaS services are who uses the service and how it is being used.

In addition to these two external factors, some inherent characteristics of SaaS services related to their functionality and deployment may surface different human rights issues and provide various degrees of leverage to address them: open vs. closed platform, volume and sensitivity of data processed, level of automation involved, level of interoperability, cloud versus on-premises, sales model, level of customizability, level of substitutability. Each of these characteristics represents a spectrum; the risk profile of a SaaS service may change based on where it falls on these spectrums.

## Human Rights Impacts

We identified five main areas of impact for B2B SaaS services:

- 1. Customer end-use:** As they are positioned further up the value chain, one of the biggest risk areas for B2B SaaS services is customer end-use. Who uses the service, which country they are in, and what they use the service for may lead to drastically different human rights impacts.
- 2. Privacy and data governance:** Most SaaS services rely on data input to serve their purpose. Which data is collected, how, and how that data is stored and used may impact the privacy of end-users and employees.

3. **Responsible AI:** Some SaaS services include artificial intelligence (AI) systems, which may amplify the risks associated with using data and algorithmic decision-making. An ethical and human rights-based approach to AI aims to address the adverse social impacts of AI usage.
4. **Content-related issues:** Some SaaS services include platforms that are open to user-generated content, or marketplaces offering integration with third-party applications. These functionalities may surface new human rights impacts related to content moderation.
5. **Worker-centered design:** SaaS services are used in a range of contexts by different types of workers. As the direct users of B2B SaaS services, workers are regularly impacted by the way in which the products are designed and deployed.

## Recommendations

SaaS providers can take the following actions to address these human rights impacts. The following recommendations should exist in a framework of ongoing human rights due diligence capable of addressing new human rights risks as the SaaS sector evolves.

1. **Avoid, prevent, and mitigate human rights harm:** Define what customers and users can and cannot do with the service, establish ways to implement these policies/terms, and define who the SaaS provider will and will not sell to, partner with, and what use cases are acceptable.
2. **Technology and design choice:** Establish technical limitations to SaaS service functionality to restrict how it can be used and/or the addition of features or customizations that have the potential for adverse impacts.
3. **Ongoing human rights due diligence:** Conduct ongoing human rights due diligence on products, platforms, and services to assess for actual and potential impacts across the full range of human rights.
4. **Transparency, guidance, and communications:** Share information about the service, best practices, and human rights-based approaches that reduce the likelihood of adverse impacts.
5. **Industry collaboration:** Collaborate with companies across the SaaS sector, stakeholders, and the broader tech industry to better understand the human rights risks of SaaS products, platforms, and services—as well as to share insights and establish overarching guidance and best practices.

# Contents

I. Introduction	5
II. Methodology	8
III. Observations on the SaaS Sector	12
IV. Human Rights Impacts	18
V. Recommendations	34

## **Acknowledgements**

This report was written by Lale Tekisalp, Faraz Ansari, and Hannah Darnton at BSR. BSR would like to thank BSR's Dunstan Allison-Hope, the members of the SaaS Human Rights Working Group, and our civil society partners for participating in the assessment and contributing to this paper.



# I. Introduction

With the massive growth of cloud computing over the last decade, companies are moving to a subscription-based software delivery model. Software-as-a-service (SaaS) makes up the largest segment of the public cloud market, with worldwide spending projected to reach US\$172 billion in 2022.<sup>4</sup> These services address numerous business needs, and power many of the consumer-facing products and platforms we use every day.

Since most business-to-business (B2B) software services do not interface with consumers, they have fewer human rights impacts than consumer-facing services such as social media platforms.

However, B2B software can also be connected to adverse human rights impacts, and B2B software providers have a role to play in ensuring that their products and services are not used in ways that lead to harm.

To further explore these impacts, BSR has been working with a group of seven SaaS companies to explore the norms, expectations, and best practices for the responsible use of SaaS services.

## **A Human Rights Assessment of the SaaS Sector**

A common theme that emerged during BSR's engagement with SaaS providers was that they often have little insight into how customers use their services—for example, for reasons of privacy.

By contrast, a common theme that emerged during BSR's engagement with external stakeholders was the need for SaaS providers to conduct due diligence to better understand their impacts.

We agree that there is a need for a deeper understanding of how SaaS services can impact human rights, the appropriate actions that SaaS providers can take to address those impacts, and dialogue among the sector to align on norms and best practices. At the same time, there are characteristics inherent in the SaaS industry that will continue to constrain insights.

Building on BSR's previous paper, "Responsible Product Use in the SaaS Sector<sup>5</sup>," we conducted a sector-wide human rights assessment of the SaaS sector focused on the use of B2B services.

This paper summarizes the results of the assessment. It identifies the SaaS sector's salient human rights risks and outlines ways in which SaaS providers may impact human rights—either as individual companies, as a group of companies, or as a sector.

In the final section of this paper, we make recommendations to SaaS providers on how to avoid, prevent, and mitigate adverse human rights impacts.

## Defining the SaaS Sector

Cloud computing allows the delivery of IT services through the internet. There are three main cloud computing service models:

- Infrastructure-as-a-service (IaaS), which allows companies to use IT infrastructure capabilities such as computing power or storage from service providers
- Platform-as-a-service (PaaS), which allows companies to use software tools to build applications, in addition to the underlying infrastructure
- Software-as-a-service (SaaS), which allows companies to use packaged software ready to run, including all the underlying infrastructure and platform capabilities

While these three service layers are interrelated, this paper focuses specifically on SaaS.

As of 2021, there were approximately 15,000 SaaS companies in the US alone, serving an estimated 14 billion customers around the world.<sup>6</sup> The SaaS products and services available address an infinite number of business needs, making it difficult to define the sector or create categories that cover the full range of SaaS offerings.

At a high level, there are two primary types of B2B SaaS services, horizontal and vertical:

- Horizontal services are industry-agnostic, addressing the needs of different types of companies. Such needs include file sharing, email, collaboration, video conferencing, data analysis, customer retention management, and human resources management.
- Vertical services address industry-specific needs. Solutions may include electronic health record (EHR) management systems for healthcare, production scheduling software for manufacturing, and learning management systems for schools, among others.<sup>7</sup>

Each SaaS service serves different business needs and therefore may impact human rights in different ways. This paper does not attempt to assess the potential impacts of every single type of SaaS service; instead, it lays out characteristics of SaaS services that may have implications for human rights.

---

## **Evolving Landscape of Responsibility**

To date, technology and human rights conversations have focused largely on consumer-facing services that may be connected to human rights harms through user-generated content on their platforms, or through privacy violations, among other issues. The connection to human rights harm can be less clear for other companies in the technology ecosystem, including cloud infrastructure providers, and of the nature of their responsibility to address adverse human rights impacts is under debate.

In recent years, the discussion around online content moderation, in particular, has focused increasingly on the lower parts of the tech stack to explore the role of such service providers in moderating content<sup>8</sup>. SaaS providers are now exploring their connection to adverse human rights impacts and their responsibility to address them in a more deliberate manner.

Notably, many companies have been exploring questions on acceptable use policies and user gating. Some have begun to take action. For example, SaaS providers such as Twilio, Okta, Slack, and Zendesk suspended services to controversial social media platform Parler for its role in enabling the January 2021 insurrection at the US Capitol<sup>9</sup>.

However, save for a few exceptions, many of the actions taken by SaaS providers to date have been ad-hoc responses to one-off cases of customer misuse or abuse. Furthermore, these measures are often based on a company's ethos or values, rather than on internationally established standards. This paper offers guidance to SaaS companies on how to establish frameworks for addressing potential adverse human rights impacts.



## II. Methodology

BSR's Human Rights Assessment (HRA) methodology<sup>10</sup> is based on the UN Guiding Principles on Business and Human Rights (UNGPs) and includes consideration of the human rights principles, standards, and methodologies upon which the UNGPs were built.

Individual company HRAs are conducted to identify and assess impacts to human rights and determine appropriate action to address those impacts. They are often undertaken to inform strategy and to position companies to fulfill their responsibility to respect human rights.

In accordance with the UNGPs, credible human rights assessments:

- Assess impacts to people, not impacts on business;
- Assess impacts against all internationally recognized human rights;
- Draw upon internal or independent external human rights expertise; and
- Highlight the concerns of affected stakeholders.<sup>11</sup>

Within these parameters, there is flexibility to determine how to conduct the assessment. This allows for adaptation to different industries, issues, and geographies while prioritizing the risks to people, rather than the risks to the business.<sup>12</sup>

This assessment builds upon existing HRA methodology<sup>13</sup> to consider the human rights impacts of a sector as a whole.

### **Sector-Wide Human Rights Assessment**

A sector-wide HRA differs from an individual company HRA in a few important ways.

First, it assesses human rights impacts not only on an individual company or product level, but also considers impacts that may arise from the cumulative actions of several companies.

Second, it allows for an assessment of the sector on a macro level, focusing on broader facets

such as dominant business models across the sector, the way the sector is organized, and the sector's potential longer-term societal and environmental impacts.

SaaS companies have tremendous potential to enable the enjoyment, realization, and fulfillment of human rights; however, in line with the UNGPs, this sector-wide assessment primarily focuses on actual and potential adverse human rights impacts and methods to address them.

For this sector-wide HRA, we considered impacts of the SaaS sector on three different levels:

- **Company-level impacts:** impacts arising from a SaaS provider's business operations, products, services, or platforms
- **Cumulative impacts:** impacts arising from, or exacerbated by, the actions taken by more than one SaaS provider
- **Sector-level impacts:** impacts caused by the sector as a whole, either as a result of the SaaS business model or the way the sector is organized.

Previous sector-wide HRAs, such as those undertaken by the Danish Institute for Human Rights<sup>14</sup>, have mostly focused on the impacts of a sector in a specific geographic area. This HRA is different in that it does not have a specific geographic focus, but rather considers impacts of the SaaS sector across markets and across a wide range of potential customers.

Finally, by assessing the impacts of the SaaS business model as sector-level impacts, we aim to contribute to the field's overarching approach to assessing business models.



This sector-wide HRA assesses human rights impacts not only on an individual company or product level, but also considers impacts that may arise from the cumulative actions of several companies.

## Identification and Prioritization

BSR uses the international legal human rights framework as the basis for defining the scope of the term “human rights.” Companies today are expected to respect all human rights, and it is understood that businesses can potentially impact any of them. Therefore, BSR uses as its baseline the universe of rights codified in the International Bill of Human Rights (The Universal Declaration of Human Rights, The International Covenant on Economic, Social, and Cultural Rights, and The International Covenant on Civil and Political Rights) and other international human rights instruments as relevant.

BSR identifies actual and potential human rights impacts and the human rights risks and opportunities arising from those impacts. BSR prioritizes human rights using factors contained in Principles 14 and 24 of the UNGPs:

- **Scope:** How many people could be affected by the harm or opportunity?
- **Scale:** How grave are the impacts for the victim?
- **Remediability:** Will a remedy restore the victim to the same or equivalent position that they held before the harm?

As this is a sector-wide HRIA, we did not assess these severity factors for individual products or companies; rather, we considered the salience of a human rights impact for the SaaS sector as a whole.

## Appropriate Action

BSR considers the appropriate action for companies using factors contained in Principle 19 of the UNGPs:

- **Attribution:** How closely is the company connected to the human rights impact?
- **Leverage:** How much leverage does the company have to influence the impact?

Similar to how we assessed the severity of human rights impacts, we considered attribution and leverage for the SaaS sector as a whole and discussed how the different characteristics of SaaS services influence these factors.

## Rightsholder and Stakeholder Engagement

Effective human rights due diligence requires meaningful engagement with rightsholders whose human rights may be impacted by the company, or by working with reasonable alternatives such as independent expert resources, human rights defenders, and others from civil society. Particular attention should be paid to human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalization.

We define rightsholders and stakeholders as follows:

- **Rightsholders:** Individuals whose rights could be impacted by the company or through the use of the company's products and/or services. Rightsholders may directly interact with the company and its products and services as employees, contractors, customers, or users. However, in the context of the end-use of SaaS services, affected rightsholders may also include non-users who do not interact directly with the company or its services. For example, if a healthcare provider uses a Customer Relationship Management (CRM) solution, all beneficiaries of the healthcare service are potential rightsholders for the provider of the CRM solution.
- **Stakeholders:** Organizations informed about and capable of speaking on behalf of rightsholders, such as civil society organizations, activist groups, opinion formers, policy makers, or regulators.

In this HRA, BSR engaged directly with a range of experts and civil society organizations, who provided insights into the risks and opportunities for rightsholders arising from the use of SaaS products. To enable candid dialogue, the identities of the individuals and organizations we consulted have been kept confidential.

Engagement with rightsholders and stakeholders is particularly challenging for SaaS providers given the huge scope of rightsholders that may be impacted in the downstream value chain of SaaS services.





# III. Observations on the SaaS Sector

## Attribution to End-Use Impacts

In the context of end-use of products and services, a B2B SaaS provider can impact human rights in two main ways: (1) through their own activities (e.g., misusing data or developing biased algorithms), or (2) through the activities of their customers. For the latter, it is particularly challenging for SaaS providers to foresee the downstream human rights impacts that they may be connected to.

There are several reasons for this:

- B2B SaaS providers are typically higher up in the value chain, which distances them from impacts that might occur when a customer uses their services.
- Many B2B SaaS services are either sold through third-party distributors, resellers, or systems integrators—or customers self-sign-up for the services.
- The design and structure of B2B SaaS services are often based on customers' needs and desired privacy, and technical features may prevent the SaaS provider from knowing what their customers are doing with the service.

Consequently, SaaS providers typically have limited insight into the end-use of their services and the associated human rights impacts.

This is similar to the experience of B2B companies in other industries that are distanced from their end-users. For example, extractives companies and component manufacturers in the hardware supply chain also have low visibility about the end-use of their products and services. These include minerals extracted from the ground for the former and electronics parts for the latter. We believe that the SaaS industry can learn from other industries who have struggled with this challenge.

However, as BSR pointed out in an earlier report, “Increased public consciousness and stakeholder understanding of downstream human rights impacts, coupled with the emerging HRDD regulatory requirements, is leading to a new era in which companies must be prepared to identify, avoid, prevent, and mitigate the adverse human rights impacts associated with their products and services.”<sup>15</sup> **Due diligence related to end-use of products and services is increasingly expected from companies further up the value chain, such as providers of B2B SaaS services.**

To address their potential downstream human rights impacts, SaaS providers must determine their company’s connection to potential human rights harms. The actions that a company must take to avoid, prevent, and mitigate adverse human rights impacts depends in part on their attribution to such impacts.

According to the UNGPs, a company may cause, contribute, or be directly linked to an adverse human rights harm. The cause/contribute/directly linked framework is an important tool to help companies understand their attribution to human rights impacts.<sup>16</sup>

The United Nations B-Tech Project<sup>17</sup> builds on this framework, proposing that technology companies contribute to an impact when they:<sup>18</sup>

- **Facilitate or enable** another entity to cause an adverse impact, where a company’s actions add to the conditions that **make it possible** for use of a product by a third party to cause a harm;
- **Incentivize or motivate** another entity to cause an adverse impact, where a company’s actions **make it more likely** that a product or service will be used in ways that cause harm; or
- Fail to **undertake reasonable human rights due diligence** to identify and address harms.

SaaS providers should understand how their unique position in the value chain, and the specifics of their service offerings, affect their company’s attribution to human rights impacts. This, in turn, will help determine what actions they should take to prevent and mitigate risks.

## “Know Your Customer” Ethics

Some companies ask ethical questions about who they choose to do business with, regardless of how closely connected they are to a harm. In our engagement with SaaS providers, we saw that some providers stopped working with specific companies or industries due to values misalignment or pressure from employees, while others followed legal sanctions when it comes doing business with certain customers and partners.

As BSR pointed out in an earlier report, “While the UNGPs emphasize a specific connection between product/service and corresponding harm, some downstream business relationships can legitimize and empower bad actors to commit human rights violations in an indirect way.”<sup>19</sup> Such business relationships may create ethical conundrums and reputational risk for companies (see callout box on Reputational Risk). Although this HRA does not focus on ethical and reputational questions, companies’ increasing attention to these factors indicates that the importance of downstream due diligence is growing.

## Reputational Risk

While reputational risks are not a focus of human rights assessments, doing business with certain entities may bring significant reputational risk for SaaS providers. As long as they are connected to an entity causing harm, providers should accept the consequences of this risk.

Principle 19 of the UNGPs states: “In any case, for as long as the abuse continues and the enterprise remains in the relationship, it should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequence—reputational, financial, or legal—of the continuing connection”.<sup>20</sup>

## The SaaS Value Chain

An important part of human rights due diligence is identifying rightsholders that may be impacted, even though this may be challenging for B2B SaaS providers who have low levels of visibility into end-use of their products and services. To understand different groups of rightsholders that may be impacted adversely through the use of SaaS services, we should first look at SaaS providers’ location in the value chain.

SaaS providers sit towards the beginning of the value chain. They receive inputs from suppliers to create software service offerings, which are then made available to customers across a range of industries and geographies, either directly or via distributors, resellers, or systems integrators. Typically, customers’ employees use the services for business operations, or to create other products or services with direct impacts on other rightsholders.

### Value Chain



Human rights impacts related to the end-use of SaaS services can occur anywhere in the downstream value chain. It is important for SaaS providers to assess impacts not only on the end-user, but also on the direct user and other groups that may be impacted along the value chain. Even individuals who do not interact with a SaaS service can be impacted through the end-use of that service.

To make this more practical, we will look at three examples of SaaS providers and describe the different groups of rightsholders potentially impacted by each provider's services. We will use these examples throughout the report to illustrate potential human rights impacts.



**SaaS Service Provider 1** provides enterprise solutions, such as customer relationship management (CRM) or human capital management (HCM) services. They sell their solutions through distributors and resellers who customize the services before selling them to customers. One of their customers is a retail company. This SaaS provider's service may have an impact on the following groups:

**Customer/Direct User**

employees of the retail company (sales and marketing teams for the CRM solution, and HR teams for the HCM solution)

**End-User**

customers of the retail company (in the case of the CRM solution) or employees of the retail company (in the case of the HCM solution)

**Other potentially impacted groups**

employees of the distributor or reseller (sales teams, IT engineers)



**SaaS Service Provider 2** provides tools for software developers and product teams, such as issue tracking and code management services. One of their customers is a social media company that runs an open web platform. This SaaS provider's service may impact the following groups:

**Customer/Direct User**

employees of the social media company (software developers)

**End-User/Indirect User**

users of the social media platform

**Other potentially impacted groups**

anyone who is subject to the content posted on the social media platform



**SaaS Service Provider 3** provides industrial solutions, including AI-based factory plant management and modeling services. One of their customers is a company that manufactures airplanes and sells them to airlines. This provider's SaaS service may impact the following groups:

**Customer/Direct User**

employees of the manufacturing company (factory workers, product designers)

**End-User/Indirect User**

customers of the airline company (passengers), employees of the airline company (pilots, flight attendants)

## Differentiating Characteristics

The SaaS sector includes a wide range of different types of services. This paper does not attempt to describe the full range of SaaS offerings, but instead highlights key differentiating characteristics that may change the human rights risk profile of a particular service or its provider.

Typically, when assessing the downstream impacts of a company's products and services, we focus on the end-user and the use case.<sup>21</sup> **The most important considerations in evaluating the potential human rights impact of SaaS services are (1) who uses the service, and (2) how it is used.**

In addition to these two external factors, the inherent characteristics of SaaS services' functionality and deployment may surface different human rights issues and provide different degrees of leverage to address them. We have identified eight characteristics, but the list can be expanded.

### Functionality

- 1 Open vs. closed platform
- 2 Volume and sensitivity of data processed
- 3 Level of automation involved
- 4 Level of interoperability

### Deployment

- 5 Cloud vs. on-premises
- 6 Sales model
- 7 Level of customizability
- 8 Level of substitutability

Each of these characteristics represents a spectrum. The risk profile of a SaaS service changes based on where it falls on these spectrums. This section provides a brief description of each characteristic.

**1 Open versus closed platform:** SaaS services fall on the spectrum of open to closed platforms depending on whether content sharing is core to the service or not. The degree to which a SaaS service is open to user-generated content may surface different risks.

**2 Volume and sensitivity of data processed:** SaaS services rely on data input on varying levels. The degree to which a service processes sensitive personal data may surface different kinds of human rights impacts.

**3 Level of automation involved:** Some SaaS services incorporate machine learning (ML) and AI systems to analyze data and generate insights. The degree to which a SaaS service involves automation may lead to different kinds of human rights impacts, or it may exacerbate the severity or likelihood of certain risks.

---

**4 Level of interoperability:** The SaaS service model increases opportunities to integrate different software services. For some SaaS services, interoperability with other apps is an important feature that may surface new risks.

---

**5 Cloud versus on-premises deployment:** Although the definition of software-as-a-service suggests a cloud-based service model, some SaaS providers provide the option of deploying their software on-premises as well. Whether a service is cloud-hosted or on-premises surfaces different issues and offers different degrees of leverage to address them.

---

**6 Sales model:** SaaS providers employ a variety of sales models depending on the size of the customer, the geographical location, and the level of customization needed for the product or service. A crucial differentiating factor for determining risk is the degree to which providers interface with their customers before and after sales.

---

**7 Level of customizability:** SaaS providers provide varying levels of customizability—some software is ready made, whereas some allows the customer to change the code. A SaaS service’s customizability may have implications for its connection to harm.

---

**8 Level of substitutability:** Some SaaS services are more difficult to substitute than others due to their unique functionality, their “stickiness,” or their switching costs. Typically, the level of substitutability correlates with the SaaS provider’s market power. The degree to which SaaS services are interchangeable may affect how much leverage the SaaS provider has to address potential human rights harms.<sup>22</sup>

---

In the following section, we discuss how these characteristics influence the severity, likelihood, and management of human rights impacts.

# IV. Human Rights Impacts

This section includes human rights impacts on three different levels, as outlined in the methodology section above.



## Company-level impacts

Impacts arising from a SaaS provider's business operations, products, services, or platforms



## Cumulative impacts

Impacts arising from, or exacerbated by, the combined use of multiple SaaS services or through the actions taken by more than one SaaS provider



## Sector-level impacts

Impacts caused by the sector as a whole, either as a result of the SaaS business model or how the sector is organized

Assessing human rights impacts on three levels allows us to identify actions that SaaS providers can take collaboratively, in addition to individual company practices, to influence a wider set of actors.

## Company-Level and Cumulative Impacts

This section of the assessment contains tables listing the potential company-level and cumulative human rights impacts identified by BSR. In accordance with the UNGPs, we have focused primarily on identifying and assessing actual or potential adverse human rights impacts.

Identifying human rights impacts for the SaaS sector proved challenging, since SaaS services and their use cases are infinitely varied. Moreover, in theory, all human rights could be impacted through the use of SaaS services—actual and potential impacts will vary significantly according to the industry vertical (e.g., healthcare, public sector, retail, financial services) in which SaaS services are deployed. Therefore, we focused only on the human rights impacts most salient for most of the sector.

Five main impact areas are highly relevant to B2B SaaS services:

1. Customer end-use
2. Privacy and data governance
3. Responsible AI
4. Content-related issues
5. Worker-centered design

While we have segmented impacts into different categories, it should be noted that these impact areas and the relevant human rights are highly interdependent and interrelated; the improvement or deprivation of one right significantly affects the others.

For each impact area, we have outlined potential company-level and cumulative impacts and listed the relevant international human rights instruments. In the final section of each table, we have assessed the severity of the impacts, as well as the management factors. Since we cannot assess severity and management factors for every SaaS service, we have used the SaaS differentiating characteristics outlined in Section 3 to describe how these characteristics might influence the severity and management of the impacts.

To illustrate how human rights impacts may manifest across the SaaS sector, we will use the three hypothetical examples of SaaS providers outlined earlier. Again, they are:

-  **SaaS Provider One** provides enterprise software solutions, such as customer relationship management (CRM) or human capital management (HCM) services.
-  **SaaS Provider Two** provides tools for software developers and product teams, such as issue tracking and code management services.
-  **SaaS Provider Three** provides industrial solutions, including AI-based plant management and modeling services.

SaaS services are infinitely varied, and they serve a large number of different use cases. While the above list is certainly not exhaustive, these examples allow us to consider how SaaS providers and their services may be connected to human rights impacts. SaaS providers may use these examples as a starting point when examining the potential impacts of their services.

## Customer End-Use

As they are positioned further up the value chain, the biggest risk area for B2B SaaS services is customer end-use. The end user of the service, which country they are in, and what they use the service for may lead to drastically different human rights impacts.

Customer end-use encompasses the following factors: (1) the user of the service, including the company, industry, and geography, and (2) the use case.



### Company-Level Impacts

- Businesses or governments may intentionally or unintentionally misuse SaaS services in ways that violate human rights.
- Entities may use SaaS services in ways that enable the advancement of industries that harm the planet and society.
- When used in high-risk contexts or markets, SaaS services may exacerbate all the impacts listed in this section.

### Examples of Company-Level Impacts

- 👤 **SaaS Provider One:** Government entities may use a CRM solution to surveil citizens. In a country with an authoritarian government and weak rule of law, this may create significant human rights risks which would not be present in the absence of the SaaS service.
- 🔗 **SaaS Provider Two:** A company may use a software development tool to develop a messaging platform that is used by a malicious group to organize violent activities.
- 🔗 **SaaS Provider Three:** A company may use an industrial modeling solution to create an oil rig, without any attempts to disrupt the ways in which the fossil fuel industry works; alternatively the solution could be used to create weapons.

### Cumulative Impacts

- When integrated with other SaaS services, the combined use of technologies may lead to new ways of misuse that lead to human rights impacts.
- When a group of SaaS providers decides not to work with a certain company or government, the following unintended consequences may result:
  - The company or government may choose to use less rights-respecting technology.
  - This decision may have impacts on the right to access scientific advancement and its benefits.

- Limiting access to enabling services may restrict access to other critical products that depend on those services and have significant impacts on individuals' rights.
- The decision not to provide services to a specific company, government, or market may impact the rights of workers whose jobs are dependent on that service (i.e., the workforce that has been formed around a specific SaaS service) and impact economic opportunity.

## Relevant Human Rights Instruments

Depending on what use case or purpose it is used for, a SaaS service can impact all human rights. Therefore, all of the rights enumerated in the International Bill of Human Rights are in scope for impacts that may arise from customer end-use. Relevant human rights instruments include:

- The Universal Declaration of Human Rights and its implementing treaties
- The International Covenant on Civil and Political Rights
- The International Covenant on Economic, Social and Cultural Rights
- The International Labour Organization Declaration of Fundamental Principles and Rights at Work

## Assessment of Severity and Management Factors

Because it is impossible to assess the severity and management factors for an individual SaaS service without knowing the specificities of the service or its use cases, we focus on the salience of the human rights issue for the sector as a whole. We also discuss how different characteristics of SaaS services may influence the likelihood and management of impacts.

**Severity:** Impacts related to customer end-use are arguably most salient for the SaaS sector. This impact area is relevant for all types of SaaS services, and the scope includes all SaaS end-users. The scale of impact can be very high depending on the specific use case, and impacts are not always remediable.

**Likelihood and Management Factors:** The likelihood and management of impacts related to customer end-use may change based on different characteristics<sup>23</sup>, such as:

- **Level of interoperability:** If a SaaS service can easily be integrated with others, the combined use of these services may increase the likelihood of human rights impacts, and they may be less foreseeable by the SaaS provider. Interoperability also reduces technological barriers to integration for complicated software processes, such as facial recognition, making it easier for users to access or deploy capabilities such as surveillance activities, which may increase the likelihood of human rights violations.
- **Cloud versus on-premises deployment:** SaaS cloud services are likely more easily integrated with other services than on-premises solutions, increasing the likelihood of risk. However, cloud deployment models also offer greater visibility into customer use; therefore, risks related to end-use are arguably more foreseeable in cloud deployments. This indicates that when software is deployed on the cloud, the provider is more closely connected to potential human rights impacts. Furthermore, in cloud deployments, SaaS providers are responsible for the management of the software, giving them greater leverage to address potential impacts.

- **Sales model:** SaaS services with a high-touch sales model involve greater customer engagement, giving the SaaS provider more opportunity to undertake customer due diligence. This, in turn, decreases the likelihood of potential human rights harms related to customer end-use. With more customer engagement, SaaS providers have higher visibility into customer use cases, making potential harms more foreseeable. This would more closely connect SaaS providers to potential human rights impacts and give them more leverage to address them.
- **Level of customizability:** Highly customizable SaaS services are more likely to be connected to harm since customers can change the services' functionality and outcomes, making potential harms less foreseeable by the SaaS provider. This may indicate that providers have less leverage to address potential impacts. On the flip side, if a SaaS service has been customized for the specific needs of a specific company, switching costs may increase, indicating increased leverage for the SaaS provider to address potential impacts.
- **Level of substitutability:** If a SaaS service is less substitutable, the SaaS provider has higher leverage to address potential human rights harms associated with the use of their service.

## Privacy and Data Governance

Most SaaS services rely on data input to serve their purpose. What and how data is collected, how it is stored, used, and shared may impact the privacy of end-users and employees.



### Company-Level Impacts

- The use of SaaS services by a company or government entity may result in the capture of more information than is necessary. For example, SaaS services may collect personal attributes from data subjects, potentially leading to violations of privacy and non-discrimination, among others.
- The data collected for a SaaS service may be combined with other data (e.g., user information that the company already has), enabling them to gather information on individuals that could be used for surveillance.
- Law enforcement agencies may demand that SaaS providers share sensitive user data to help the agencies. Law enforcement may subsequently use this data to identify, track, or monitor individuals, which may result in a violation of individuals' rights. These risks may change depending on datacenter locations and data localization regulations.

### Examples of Company-Level Impacts

- **SaaS Provider One:** A company may use a CRM solution to collect data on race, ethnicity, socioeconomic class, or other protected category, which may then be used to discriminate against certain individuals or populations.

- ◀▶ **SaaS Provider Two:** A government entity may use a software development tool to develop spyware that is used for the surveillance of activists, journalists, and political opponents.
- ▶▶ **SaaS Provider Three:** Companies may use plant operations management software to collect data on worker performance, which may then be used to discriminate against certain groups of employees or violate employees' rights to free association.

## Cumulative Impacts

- The general increase in the use of SaaS services and the digitization of business processes may lead companies and government entities to collect more data than they otherwise would. The increased collection of data may lead to heightened privacy and cybersecurity risks, both for SaaS providers and their customers.

## Relevant Human Rights Instruments

Relevant human rights for this impact area include, but are not limited to:

- **Right to privacy:** Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." As privacy is an enabling right, the violation of privacy may have secondary impacts on other rights, including the right to life, liberty, and security, and freedom from arbitrary arrest.
- **Right to non-discrimination:** Article 2 of the UDHR states that "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."
- **Right to freedom of expression and to seek information:** Article 19 of the UDHR states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
- **Right to life, liberty, and security:** Article 3 of the UDHR states that "Everyone has the right to life, liberty and security of person."
- **Right to freedom of association:** Article 20 of the UDHR states that "Everyone has the right to freedom of peaceful assembly and association."

## Assessment of Severity and Management Factors

**Severity:** Privacy and data governance is an impact area relevant to all SaaS providers. Therefore, the scope of impact includes all SaaS end-users, and the scale of impact can be very high, depending on how data is handled. A potential violation of privacy may lead to secondary impacts that might not be remediable.

**Likelihood and Management Factors:** The likelihood of impacts related to privacy and data governance, and their management may change based on different characteristics<sup>23</sup>, such as:

- **Volume and sensitivity of data processed:** The likelihood of human rights harm related to privacy and data governance rises as the volume and sensitivity of the data processed by

the SaaS provider increases. Depending on where the data is stored, SaaS providers may be connected to potential human rights harms on various levels and may or may not have leverage to address them.

- **Level of interoperability:** If a SaaS service can easily be integrated with others, the combined use of these services may lead to a higher likelihood of privacy impacts. Access to personal and potentially sensitive data may increase, and the data that is collected through different SaaS services may be combined to gather information on individuals.
- **Cloud versus on-premises deployment:** When a SaaS service is deployed on-premises, access to data is well-defined and localized. While cloud solutions generally employ sophisticated encryption and data protection measures, they also increase the number of actors with access to sensitive data. Additionally, the usage of cloud solutions makes it easier to integrate different pieces of software, increasing the likelihood of risks related to privacy.
- **Level of customizability:** If a SaaS service is highly customizable, customers may add new fields of data to be collected from users, which would increase the likelihood of potential harms related to violations of privacy.

## Responsible AI

Some SaaS services incorporate AI systems, which may amplify the risks associated with the use of data and algorithmic decision making. An ethical and human rights-based approach to AI aims to address AI's adverse social impacts.



### Company-Level Impacts

- AI models used as part of SaaS services may introduce unintentional biases and lead to unfair or discriminatory outcomes for certain individuals or populations. This may happen when using biased or unrepresentative datasets when training or feeding AI models. If the SaaS provider can't explain how the AI model arrives at certain outputs, the problem can be exacerbated.
- Even when AI models are used as intended and datasets are representative and unbiased, some AI tools may still inherently cause human rights violations. For example, facial recognition solutions may be based on data collection practices that violate the right to privacy.
- AI models used in business contexts typically optimize for short-term financial goals at the expense of non-financial goals such as labor conditions and environmental sustainability. A reliance on algorithmic decision-making systems in SaaS services may lead to the privileging of certain goals over others, leading to unintended negative outcomes.
- AI models used as part of SaaS services may be used to analyze user or worker behavior, sentiment, or actions, leading to profiling individuals in ways that impact human autonomy and dignity.

- SaaS services employing AI models, especially in healthcare and robotics, may be used in ways that cause physical harm or compromise bodily security.
- AI models used as part of SaaS services may rely on the collection, aggregation, storage, or use of sensitive personal data. Poor data governance processes may violate the privacy rights of users.

### Examples of Company-Level Impacts

-  **SaaS Provider One:** A bank may use an AI-based enterprise SaaS service to facilitate individuals' access to financial services. If the AI model is trained using historical data, the outputs may lead the bank to discriminatory decisions.
-  **SaaS Provider Two:** A chat bot used as part of an issue-tracking software has been trained to respond to certain languages. The bot may not be as responsive to different vernaculars, preventing certain populations from benefiting from the service.
-  **SaaS Provider Three:** A plant operations management solution that optimizes for efficiency over other goals may unintentionally impact labor scheduling and workers' rights.

### Cumulative Impacts

- Business and government use of biased AI models may reinforce and exacerbate society's existing inequities.
- Widespread use of AI across SaaS providers without adequate explanations on how it functions, its limitations, or transparency around its use may normalize the use of AI without explanation or transparency, with subsequent impacts on a range of human rights.

### Relevant Human Rights Instruments

Relevant human rights for this impact area include, but are not limited to:

- **Right to non-discrimination:** Article 2 of the UDHR states, "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."
- **Right to desirable work:** Article 23 of the UDHR states, "Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment."
- **Human autonomy and dignity:** Article 1 of the UDHR states, "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."

### Assessment of Severity and Management Factors

**Severity:** Responsible AI is an impact area relevant for SaaS services that incorporate AI and ML systems. The scope includes SaaS end-users that interact with such systems. The scale of impact can be very high, depending on what outcomes and decisions are made using the outputs of the

AI model. Some of the secondary impacts resulting from a biased or erroneous AI model may not be remediable.

**Likelihood and Management Factors:** The likelihood of impacts related to responsible AI and their management may change based on different characteristics<sup>23</sup>, such as:

- **Volume and sensitivity of data processed:** If a SaaS service is inputting sensitive user data into its AI models, the likelihood of human rights harm is higher compared to a SaaS service that inputs machine data, for example.
- **Level of automation involved:** If a SaaS service incorporates AI and ML models, the likelihood and severity of human rights harm may be higher.

It is important to note that potential human rights impacts are related to how a customer uses the outputs of an AI model. However, the design of the AI model and the guidance the SaaS provider offers its customers are critical to those outcomes.

## Content-Related Issues

Some SaaS services include platforms that are open to user-generated content or marketplaces where they offer integration with third-party applications. These functionalities may surface new human rights impacts related to content moderation.



### Company-Level Impacts

- User-generated content posted on SaaS services may discriminate against certain individuals or populations. Online hate speech may also lead to offline violence, impacting individuals' rights to life, liberty, and security.
- SaaS providers operate in countries with varying views on their citizens' rights to free expression and access to information. Governments may ask SaaS providers to remove content from their platforms, limiting individuals' access to information. These risks may change depending on datacenter locations and data localization regulations.
- Third-party applications offered through the marketplaces of SaaS services may be used in ways that lead to adverse human rights impacts.

### Examples of Company-Level Impacts

- **SaaS Provider One:** A CRM solution offers integration with third-party applications through its marketplace. The applications include a tool that allows employees to leave private comments about clients, visible only to their coworkers, encompassing both work-related and personal characteristics.

- ◀▶ **SaaS Provider Two:** A collaboration solution that allows individuals to contribute to applications' source code may surface harmful user-generated content, which leads to offline violence.
- ▶▶ **SaaS Provider Three:** A plant management software offers internal communication functionality for factory workers and all workers can see the content posted by others. Some of the messages contain discriminatory speech, leading to the marginalization of certain groups of workers.

## Cumulative Impacts

- The removal of a specific piece of content by a group of SaaS providers, or their decision not to offer integration to a certain service, may impact freedom of expression and restrict access to information.
- If a growing number of SaaS, PaaS, and IaaS providers implement similar gating processes to address content-related issues at the same time, they may unintentionally infringe on human rights by limiting use of certain SaaS services to an entire swath of actors. This could, in turn, result in restrictions to freedom of expression, creating less room for dissent, or inhibiting downstream customers from accessing technologies that enable the realization of human rights, such as education, health, social services, or other critical goods and services.

## Relevant Human Rights Instruments

Relevant human rights for this impact area include, but are not limited to:

- **Right to freedom of expression and to seek information:** Article 19 of the UDHR states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
- **Right to non-discrimination:** Article 2 of the UDHR states, "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."
- **Right to life, liberty, and security:** Article 3 of the UDHR states, "Everyone has the right to life, liberty and security of person."
- **Right to participate in cultural life:** Article 15 of the ICESCR states that everyone has the right "to take part in cultural life."

## Assessment of Severity and Management Factors

**Severity:** Content-related issues are relevant to SaaS services that include an open platform or marketplace. Therefore, the scope of impact includes SaaS end-users that interact with such features. The scale of impact can be very high, depending on what content is surfaced. Harmful content may also lead to secondary impacts that may not be remediable.

Any SaaS provider who directly interacts with user-generated content needs to consider how they impact individuals' freedom of expression and access to information. This includes internal-facing services with limited user-generated content.

**Likelihood and Management Factors:** The likelihood of impacts related to content-related issues and their management may change based on different characteristics<sup>23</sup>, such as:

- **Open versus Closed Platform:** If the SaaS service includes an open platform where users can post content, the likelihood of human rights harm is higher compared to closed platforms.

For indirect impacts (e.g., third-party applications offered through marketplaces of SaaS services), SaaS providers need to consider if they should play a role in content moderation or if their customers/partners are responsible for addressing these impacts. If the SaaS provider opts to require their partners to put content governance processes in place, they should consider creating processes to ensure that their business partner is actually enforcing those requirements.

## Worker-Centered Design

Different types of workers use SaaS services in a range of contexts. Product design and deployment choices regularly impact the direct users of B2B SaaS services: the workers.



### Company-Level Impacts

- SaaS services that are not designed with users in mind may negatively impact workers' rights, creating undesirable work conditions or loss of economic opportunity, for example.
- The design of SaaS services may have impacts on how their users experience work life. SaaS services may shape the way that knowledge workers think and generate knowledge, which may produce or limit opportunities for creativity, leading to impacts on the freedom of opinion and human autonomy.

### Examples of Company-Level Impacts

- 👤 **SaaS Provider One:** The knowledge workers in a company use CRM software every day. The software's design shapes how these individuals think and generate knowledge.
- 🗨️ **SaaS Provider Two:** A team collaboration solution for software developers lacks basic accessibility features. Therefore, individuals with disabilities or those that speak different languages can't collaborate with their coworkers, hindering their job performance.
- 🔗 **SaaS Provider Three:** An AI-driven plant operations management software has not been designed with lower-level technical workers in mind. The company fires some of these technicians assuming they are not needed anymore, since most workflows will be automated. The remaining technicians have to work longer hours to adapt to the changing work conditions without any training.

## Cumulative Impacts

- Automation of business processes through the increased use of AI models may lead to job loss and other adverse impacts on workers.

## Relevant Human Rights Instruments

Relevant human rights for this impact area include, but are not limited to:

- **Right to desirable work:** Article 23 of the UDHR states, “Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment.”
- **Right to non-discrimination:** Article 2 of the UDHR states, “Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.”
- **Human autonomy and dignity:** Article 1 of the UDHR states, “All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.”
- **Right to freedom of thought:** Article 18 of the UDHR states, “Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.”

## Assessment of Severity and Management Factors

**Severity:** Worker-centered design issues are relevant for all B2B SaaS services; the scope of impact includes all direct users of SaaS services. Depending on the impact, its scale can be high, and some impacts may not be remediable.

**Likelihood and management factors:** The likelihood of impacts related to worker-centered design issues and their management may change based on different characteristics:

- **Level of automation involved:** AI and ML technologies can amplify the impacts on workers. Consequently, when a SaaS service incorporates automation, the likelihood of risk increases.

**Note on attribution:** SaaS providers would be more closely connected to impacts on workers, who are the direct users of their service, compared to impacts on end-users.

## Sector-Level Impacts

Cloud computing, the provision of IT services through shared datacenters via the internet, has had groundbreaking impacts, some of which are directly relevant to human rights. In this section, we assess the impacts of the cloud business model. Although we specifically focus on SaaS, most of the impacts can be extrapolated to cloud computing more broadly to include other cloud service models (i.e., IaaS and PaaS). While each SaaS provider and each SaaS service has its own business model, we focus on the business model elements most often adopted in the SaaS sector.

The UN Human Rights Office of the High Commissioner's B-Tech Project outlines three elements of business models: value proposition, value chain, and revenue structure.<sup>24</sup> In this section, we categorize impacts under these three buckets. We structured company-level and cumulative impacts differently; in this section, we focus on opportunities in addition to risks. We believe that the SaaS business model presents opportunities for advancing human rights, and the sector should go beyond mitigating the human rights risks to which they may be connected, and to consider how they can promote human rights.<sup>25</sup>

### Impacts Related to the SaaS Value Proposition

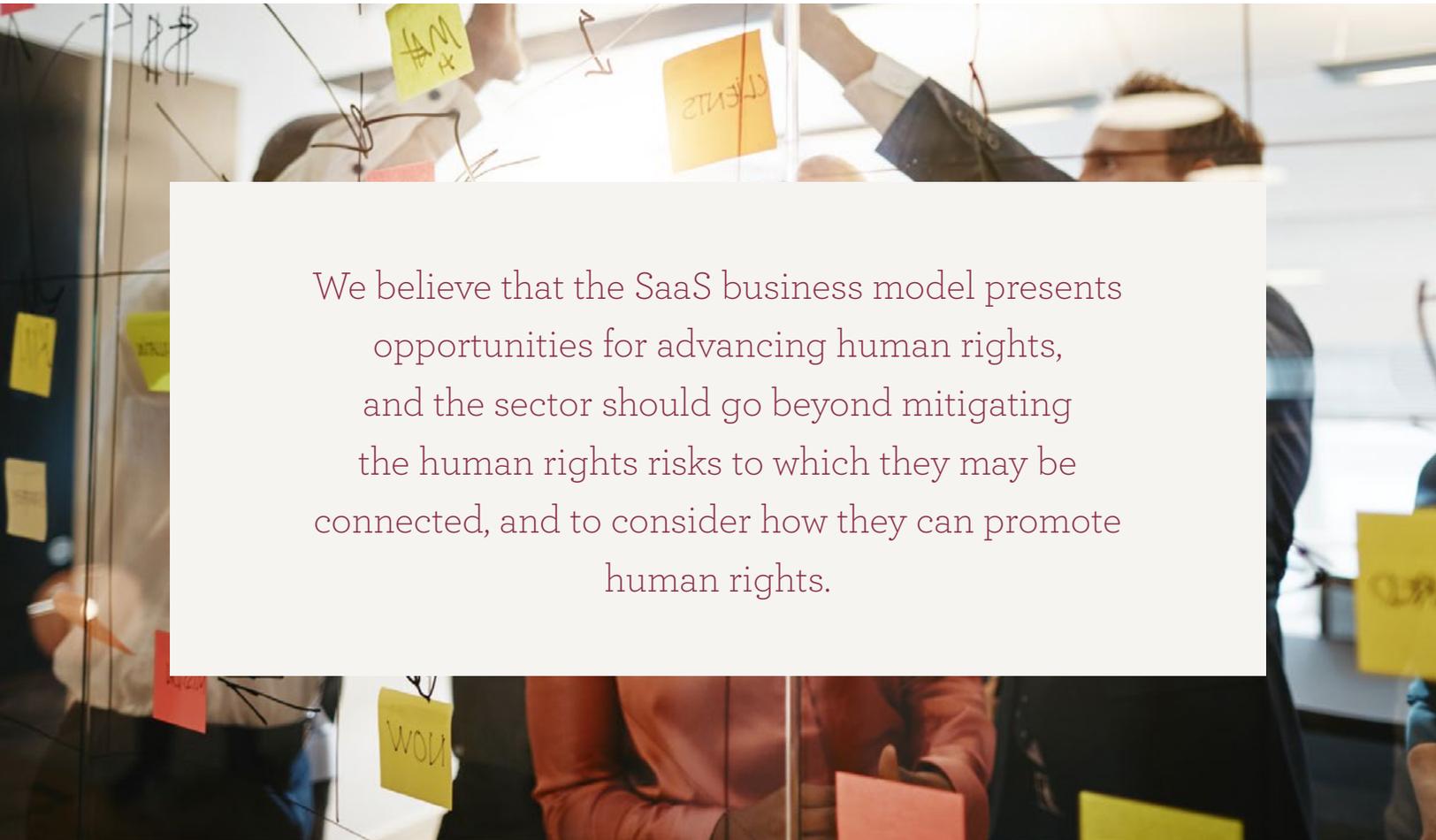
The SaaS business model's main benefits to an organization can be summarized as follows: fast provision of IT services, ability to scale services on demand, increased availability of services, less maintenance required, and increased data security. The SaaS value proposition leads to several broad human rights impacts:

- **Access to technology:** The SaaS model enables dramatically easier access to software by businesses of all sizes. Small and medium enterprises who previously could not use the latest technology due to price or availability now benefit from cutting-edge advancements. This has significant positive impacts on several rights, including the right to benefit from advancements in science and technology, the right to desirable work, and the right to participate in the cultural life of the community.
- **IT labor impacts:** The SaaS cloud delivery model requires much less IT overhead for companies, since SaaS providers manage most layers of the tech stack. This may lead to shifts in the labor market.
- **Availability of critical services:** The SaaS model allows services to function with less downtime and high availability. Even during power outages and natural disasters, SaaS services can be easily recovered. Therefore, the SaaS model gives individuals access to critical services with much less interruption, leading to positive human rights impacts.
- **Data security:** Most SaaS providers incorporate data security measures that small businesses would otherwise not be able to implement. Therefore, the SaaS model enables increased data security compared to on-premises deployments. On the flip side, having data reside in a handful of companies' datacenters creates new data security challenges. These will be assessed in the next section, which discusses value chain impacts.

## Impacts Related to the SaaS Value Chain

The SaaS value chain includes different actors such as technology suppliers, IaaS and PaaS providers, SaaS providers, their customers, and the end-users of the SaaS services. Several high-level impacts relate to the specificities of this value chain:

- **Data hosting and localization:** With the SaaS model, data is hosted on the SaaS providers' servers, instead of the servers of the company or government entity using the service. If the SaaS provider does not maintain its own infrastructure, they may also use the servers of other cloud service providers such as, Amazon Web Services, Microsoft Azure, Google Cloud Platform, or Digital Ocean. This model places increased responsibility on cloud providers to secure the data they host and to establish guardrails to protect privacy. That said, providers place most of the responsibility for privacy compliance on their customers. Moreover, the location of these datacenters has contributed to jurisdictional risks. Increasingly, governments require cloud providers to host data within their jurisdictions, which has concerning implications for government surveillance and overreach.
- **Integration with other cloud services:** The SaaS model has increased opportunities to integrate different software services with each other—either with services from the same provider, or from other providers. Offering integration to other services through appli-



We believe that the SaaS business model presents opportunities for advancing human rights, and the sector should go beyond mitigating the human rights risks to which they may be connected, and to consider how they can promote human rights.

cation programming interfaces (APIs) is an important competitive advantage for a SaaS provider as it accelerates adoption of the service and makes it more “sticky.” Increased interoperability between SaaS services and customers’ ability to use them in combination may create additional human rights impacts that should be considered.

- **Shared responsibility:** The move to cloud computing has changed the division of labor between the customer and the service provider. With on-premises deployments, customers need to manage most layers of the tech stack, but with cloud deployments, providers are more responsible for managing those layers. With SaaS, providers manage all layers while customers simply consume the packaged end product. In the case of a potential human rights harm, the SaaS provider may be more closely related to the harm than they would be in an on-premises deployment, with more leverage to address the harm.
- **Indirect sales channel:** Many SaaS companies rely on indirect sales channels to sell their products more widely—especially in jurisdictions where they don’t have their own operations, which often includes countries with a weaker rule of law and fewer human rights protections. Sales channels often involve several entities and tracing the path of a produced product to the end customer can be challenging. Often, products and services from multiple companies are integrated at the endpoint, so it can be challenging to anticipate use cases. Sales partners are incentivized to make sales, and providers face pushback from partners against time-consuming due diligence requirements, particularly if partners feel they cannot increase prices to compensate for the additional administrative burden.
- **Environmental impacts:** The increased use of computing power through SaaS providers’ datacenters may have negative environmental impacts that could lead to adverse human rights impacts.

## Impacts Related to the SaaS Revenue Structure

The SaaS revenue structure relies largely on subscription-based ongoing payments. Some SaaS providers also charge for additional functionality, reporting, setup, or customer service. The different SaaS revenue and pricing models may have impacts on human rights, as well as human rights due diligence practices undertaken by companies:

- **Faster provision of services and the ability to scale on demand:** Most SaaS services rely on a pay-as-you-go model in which customers pay based on their usage. Since there is no upfront cost, customers can start using a service much faster and scale their usage on demand. This model has significant positive human rights impacts by creating easier access to technology. On the other hand, this pricing model may also allow risky products or business models to scale up rapidly without proper due diligence and have impacts that are disproportionate to their revenue and head count.<sup>26</sup>
- **Continuous engagement between provider and customer:** Once a SaaS provider acquires a new customer, the provider tries to expand their revenue from that customer by upselling new services or functionality. This allows for continuous engagement between the SaaS provider and its customers, which may have advantages for ongoing human rights due diligence. The continuous nature of a subscription-based revenue structure indicates that SaaS providers may have increased leverage to address potential human rights impacts, as they can more easily disable customers from receiving their services.

- **Ability to limit features:** Many SaaS services have a plan-based pricing structure in which different plans include different features. Some providers offer a “freemium” model in which the customer begins with a free plan with limited features. Those clients can opt to pay for some of the premium features. This allows SaaS providers to limit the use of some of the potentially riskier features, which may have advantages for human rights due diligence.

## Vulnerable Groups

Companies should pay particular attention to the rights, needs, and challenges of individuals from groups or populations that may be at heightened risk of becoming vulnerable. Vulnerable groups are those that face marginalization, discrimination, or exposure to other adverse human rights impacts with greater severity and/or less potential for remediation than others.

Vulnerability depends on context. Someone who may be powerful in one context may be vulnerable in another. Examples include:

- **Formal discrimination:** laws or policies that favor one group over another
- **Societal discrimination:** cultural or social practices that marginalize some and favor others
- **Practical discrimination:** marginalization due to life circumstances, such as poverty
- **Hidden groups:** people, such as undocumented migrants, who might need to remain hidden and consequently may not speak up for their rights

SaaS providers should endeavor to identify vulnerable groups whose rights, needs, and challenges require extra attention during the design, growth, and development of their services.

In the context of end-use, SaaS services may impact different groups of rightsholders. As outlined in section three of this report, these groups include, but are not limited to, the direct user of the service and the end-user. Other “non-user” groups of rightsholders may also experience impacts along the downstream value chain of the SaaS service.

# V. Recommendations

According to the UNGPs, appropriate action to address potential adverse human rights impacts varies according to: (1) whether a company “causes” or “contributes” to an adverse impact, or whether it is involved solely because the impact is “directly linked” to its operations, products or services by a business relationship; and (2) the extent of its leverage in addressing the adverse impact.

Where a company would cause a potential adverse impact, it should take the necessary steps to cease, avoid, or prevent it. Where a company would contribute to a potential adverse impact, it should take the necessary steps to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible. Where a company would be directly linked to an impact, it should use leverage to prevent or mitigate the impact and consider ending the relevant business relationship(s).<sup>27</sup>

In the context of this assessment, a cause, contribute, and directly linked conclusion will vary from company to company, and case by case.

However, regardless of a cause, contribute, or directly linked conclusion, a human rights-based approach should be taken.

A human rights-based approach (HRBA) applies the principles and methodologies that underpin (and pre-date) the UNGPs, such as accountability, non-discrimination, and equality, transparency, vulnerability, participation, and informed consent, as well as the principles of legitimacy, necessity, and proportionality, independent of a company’s precise connection to a harm.

Furthermore, in situations where rights are in tension (e.g., freedom of movement versus bodily integrity), companies will need to deploy an HRBA to decide how to pursue the fullest possible expression of both rights.

Appropriate action to address adverse impacts can be categorized as follows<sup>28</sup>:

- **Avoid, prevent, and mitigate human rights harm:** Take action to define what customers and users can and cannot do with the service, establish mechanisms to implement the policies and terms, and define who the SaaS provider will and will not sell to, or partner with, and what use cases are acceptable.
- **Technology and design choice:** Establish technical limitations to SaaS service functionality to restrict how it can be used and/or the addition of features or customizations that have the potential for adverse impacts.
- **Ongoing human rights due diligence:** Conduct ongoing human rights due diligence on products, platforms, and services to assess for actual and potential impacts across the full range of human rights.
- **Transparency, guidance, and communications:** Share information about the service, best practices, and human rights-based approaches that reduce the likelihood of adverse impacts.
- **Industry collaboration:** Collaborate with companies across the SaaS sector, stakeholders, and the broader tech industry to better understand the human rights risks of SaaS products, platforms, and services; share insights; and establish overarching guidance and best practices.

These five approaches should exist in a framework of ongoing human rights due diligence capable of addressing new human rights risks as technology, and the SaaS sector overwhelmingly, evolve.

## 1. Avoid, Prevent, and Mitigate Human Rights Harms

Take action to define what customers and users can and cannot do with a SaaS provider's service, establish mechanisms to implement the policies/terms, and define who the provider will and will not sell to, partner with, and what use cases are acceptable. Companies can begin to do this through the following actions:

### **AUPs and Service Specific Terms**

Deploy, and ideally publish, an Acceptable Use Policy (AUP) that describes the intended use of the SaaS service; the prohibited uses, content or activity; and the company's enforcement practices.<sup>29</sup> Public AUPs set clear expectations for customer use and provide a clear basis for enforcement actions when the policy is violated.

In addition to the AUP, deploy tailored service-specific terms for individual products and services that restrict how they are used and address risks specific to that service. SaaS providers could also consider including service termination clauses in the case of severe human rights violations by customers.

### **Customer Gating**

Institute a "gating process" for prospective SaaS customers. The gating process is intended to help companies establish boundaries and limitations on who they will and will not do business with and consider how they will implement these limitations.

Gating processes can be applied at an industry or customer level. An industry-based approach identifies the characteristics of high-risk industries or industries where the SaaS product or service is likely to be connected to a harm. These characteristics then inform the development of criteria that determine which industries the company will or will not work with. Gun manufacturers or providers of hacking tools might be an example.

A customer-based approach to gating identifies customer characteristics, behaviors, use cases, or markets that are likely to be connected to human rights harms and informs who the company will or will not sell to. A company with a history of causing human rights violations might be an example.

Regardless of approach, gating processes should be formalized and consistently applied across prospective customers, rather than implemented ad hoc. They should be based on established international human rights standards and norms. Guiding questions to help companies establish boundaries on who they will and will not do business with, and how to implement these limitations, can be found in the paper, “Responsible Product Use in the SaaS Sector.”

---

While gating can help avoid and prevent human rights harms, it should be implemented with caution.

---

While gating can help avoid and prevent human rights harms, it should be implemented with caution.

As mentioned in the human rights impacts section above, if a growing number of SaaS, PaaS, and IaaS providers implement similar gating processes at the same time, they may unintentionally yet systematically infringe on human rights by limiting use of the technology to an entire swath of actors. This could, in turn, result in restrictions to freedom of expression, creating less room for dissent, or inhibiting downstream customers from accessing technologies that enable the realization of human rights, such as education, health, social services, or other critical goods and services. Examples might include SaaS providers creating gating processes that restrict or ban customers with platforms allowing “awful but lawful” speech, or civil service departments in high-risk countries (such as Afghanistan or Myanmar) where public services continue to play a vital role.

Gating processes are often most suited to situations where the company is delivering customized solutions for customers; however, a customer self-gating process (or online form) could also be deployed before the sale of less customized products and solutions,

such as general-purpose tools openly available for purchase online. To institute gating approaches at scale, companies may want to consider two options:

- i. **Gating undertaken by the SaaS provider before a sale:** This could include assessments of public human rights commitments, company human rights rating and rankings, nature of company ownership, countries of concern, high-risk application areas, and nature of the intended use of the SaaS product or service. This approach could involve an escalation process for potentially concerning sales. It would be most suited to situations in which the SaaS provider is delivering customized solutions for customers.
- ii. **Customer-led gating process before a sale:** This could include requirements that the customer would need to fulfill before obtaining rights to use the product or service, such as agreeing to service-specific terms, undertaking human rights training, agreeing to implement an opt-out or opt-in process, and/or establishing a reporting channel.

## 2. Technology and Design Choice

Establish technical limitations to SaaS service functionality to restrict how it can be used and/or the addition of features or customizations that have the potential for adverse impacts. Companies can begin to do this by taking the following actions:

### **Assess Data Sets and Data Sources to Avoid or Reduce Bias**

Conduct systematic reviews and vet training data as part of the due diligence process. This includes reviewing data sets for adherence to internal responsible data principles, guidelines, or best practices from external sources.

When relevant, internal processes and procedures should also include checks on whether proposed data sources for AI solutions are reputable and not affiliated with political or special interest groups; assessments on whether the data is representative of vulnerable or marginalized populations; use of techniques that train models evenly despite the use of biased datasets by re-weighting the data; creation of and adherence to guidelines on unbiased data selection for employees.

### **Adversarial Testing**

Require parties involved in the design, development, and use of the SaaS product or service to conduct stress testing or adversarial testing to identify potential technological errors, ways in which the service could be misused or abused, or ways in which the use case could result in adverse human rights impacts. Consider bringing in external experts and stakeholders to assist with this process.

This could also be conducted in collaboration with customers as part of the product development or proof of concept process for customized platforms, services, or products.

SaaS providers can integrate futures methodology and strategic foresight into adversarial tests to consider how SaaS services and the context in which they are deployed may change and evolve over time. It is important to consider a wide range of potential impacts that might arise in the future, and not be constrained by human rights impacts that are well known today.

### 3. Human Rights Due Diligence

Companies should conduct ongoing human rights due diligence on products, platforms, and services to assess for actual and potential impacts across the full range of human rights. Companies can begin to do this by taking the following actions:

#### **Undertake Ongoing Human Rights Due Diligence**

As SaaS products and services and the context in which they are used will inevitably change, human rights due diligence should be ongoing and consider shifts in customers, markets, and use cases to identify actual and potential human rights impacts over time.

Human rights due diligence focuses on identifying risks to people rather than risks to the business and requires engaging with and paying special attention to the rights and needs of individuals from groups or populations that may be at heightened risk of vulnerability.

While this may be difficult in the SaaS context, SaaS providers should work to engage rightsholders or their representatives, or work with industry collaborations that can help provide insights and feedback from potentially impacted groups on the products and services in question.

---

Due diligence should be carried across the life cycle of technology—the research, design, development, sale, and use phases.

---

Due diligence should be carried across the life cycle of technology—the research, design, development, sale, and use phases.

#### **Establish Relationships with Customers**

When possible, establish partnership-based relationships with SaaS customers. This will allow SaaS providers further insight into how customers use the service in practice and may facilitate risk identification and mitigation.

This could include regular meetings (e.g., annually) about their use of SaaS tools and features, particularly with the teams and individuals interacting directly with the solution and familiar with the spectrum of use cases.

This may be more feasible with customized offerings where the SaaS provider, customer, and/or partner work hand-in-hand on the design and development of a service, or where updates and ongoing maintenance or services are required.

Customer relationship building and human rights due diligence can be prioritized based on the severity and likelihood of the human rights risks of the customer.

### **High-Risk Markets**

Make an informed decision on whether entry into a certain market is consistent with a human rights-based approach.

This could involve reviewing prioritized data sources<sup>30</sup> to gauge the level of human rights risks across prospective markets. Quantitative rankings will allow the company to more easily identify, prioritize, and address actual and potential human rights impacts associated with markets where either they, or their customers, are working.

---

Quantitative rankings should be considered in tandem with qualitative data sources. Qualitative data sources (such as annual human rights reports by the State Department, Amnesty International, Human Rights Watch, and Freedom House) provide essential analysis for fully understanding the human rights context in a country.

---

Quantitative rankings should be considered in tandem with qualitative data sources. Qualitative data sources (such as annual human rights reports by the State Department, Amnesty International, Human Rights Watch, and Freedom House) provide essential analysis for fully understanding the human rights context in a country.

The sale of the product or service for use in countries that are found to be high-risk can be escalated for further review. If found that the use of the product or service has the potential to be connected to a harm, the company could either seek to mitigate the potential harms associated with the deal (e.g. through restricted service features, a robust AUP, ongoing customer dialogue and training, and ongoing human rights due diligence) or decide not to make the sale.

From a human rights perspective, selling into a high-risk market without addressing the actual and potential human rights impacts is not an option—this approach would not be consistent with the company’s responsibilities under the UNGPs.

However, high-risk markets are often the very places that will benefit most from SaaS products deployed in the service of public good. For this reason, SaaS companies should take nuanced approaches, such as prioritizing specific industry verticals as they enter new markets or seeking to use market presence to urge human rights and rule of law reform. Human rights outcomes may not be best served by SaaS companies avoiding higher-risk markets en masse.

If the SaaS provider discovers that they have unintentionally entered a market that has been designated as high-risk via a customer, or the risk categorization of an existing market has increased to high-risk, the SaaS provider should undertake due diligence to evaluate the human rights risks associated with remaining in country or exiting and take action accordingly. Should the SaaS provider opt to continue serving the market in question, it should take action to avoid, prevent, and mitigate identified human rights risks. If the provider decides to exit the market or business relationship in question, it should take efforts to avoid, prevent, and mitigate the adverse human rights impacts of ceasing the relationship, including impacts to the partner company, their clients, workers or employees, and local community.

### **Transparency, Guidance, and Communications**

As part of their efforts to prevent, avoid, and mitigate adverse human rights impacts, SaaS companies should communicate their commitment to human rights publicly and disclose information that will educate the broader public on human rights risks and opportunities.

### **Human Rights Policy**

Publish a clear commitment to human rights. This should include a description of how the company evaluates human rights impacts of the product or service, the risks associated with customers and end-use of the SaaS service, and the actions they have taken to address these risks.

### **Training and Guidance on Human Rights**

SaaS companies should provide training and guidance on the intended use of the product, platform, or services to their employees, customers, and partners. This should include educational content on each technology or service offering, a description of intended use cases, limitations, best practice guidelines, and in-product guidance.

These materials could also be accompanied by supplemental platforms such as employee, customer, or user forums. Training and guidance should highlight acceptable use of the product or service and note any product or service limitations that could result in human rights harms.

SaaS companies may also want to include training or educational materials on the risks that may arise with specific SaaS product or service features, such as user-generated content or personal data collection, aggregation, storage, or sharing.

Trainings should be designed to raise awareness of potential adverse human rights impacts. Training and guidance will be most impactful if the customer has a company-wide integrated approach to human rights and ethical use.

While these soft interventions may lack the legal force of AUPs and service terms, stakeholders have emphasized the importance of training, guidance, and best-practice sharing in changing behavior and addressing human rights risks.

While these soft interventions may lack the legal force of AUPs and service terms, stakeholders have emphasized the importance of training, guidance, and best-practice sharing in changing behavior and addressing human rights risks.

Internally, SaaS companies can encourage the socialization and discussion of human rights issues by creating programs such as ethical debate clubs, human rights and ethics champs, or human rights office hours.<sup>31</sup>

### **Consider Publishing a List of Public Sector Customers**

Consider publishing a list of public sector customers. Many of the salient human rights impacts arising from the use of SaaS services occur during their application by public sector customers who have their own duty to protect human rights. SaaS providers should review the pros and cons of publishing a list of public sector customers. Such a list would be intended to provide external stakeholders with the information they need to hold government actors accountable for adverse human rights impacts that may arise from the use of SaaS products and services.

### **Reporting Channel**

Reporting channels and grievance mechanisms provide a medium through which employees, customers, users, and other rightsholders can raise concerns related to the misuse or abuse of a company's platform, products or services, and related grievances. Reporting channels can also provide visibility into product use cases and act as an early warning mechanism for issues that may become more significant over time. Instituting these mechanisms helps accomplish two goals:

- i. **Provide a channel** for anyone to surface instances of product or service misuse and abuse
- ii. **Create an operational grievance mechanism** where an aggrieved party can seek remedy for a harm

In practice, a single channel or mechanism may serve both purposes; however, it is important to note that there are two distinct uses.

Reporting channels are an important complement to AUPs and a significant mechanism to identify non-compliance. While many companies have hotlines or ethics lines for internal employees, very few have channels specifically designed to receive feedback on how their products and services are being used, or more specifically, if they are being misused or abused.

Companies should consider who should host the reporting channel (e.g., the SaaS provider, the customer or company deploying the technology, or both), and what types of reports might be reasonably anticipated on each.

---

We recommend that each company establish its own reporting channel or integrate external reporting mechanisms into existing hotlines and “speak up” channels. Key characteristics of these reporting channels, based on international best practice (such as principle 31 of the UNGPs), include:

**Accessible:** known by those for whose use they are intended; with language, accessibility, prominence, and other factors considered

**Predictable:** provide known procedures with clear communications with the reporter at each stage

**Equitable:** clear information and guidance on how to use

**Source of learning:** gain insights into misuse to improve AUPs, gating, etc.

---

## Transparency Reports

SaaS companies have reported limited interaction with law enforcement agencies today; however, global trends show increased government demands for data from a wider range of companies.

Responding to overly broad law enforcement requests for user data could raise human rights concerns, especially when those requests come from countries with weak rule of law or poor human rights track records.

Companies receiving law enforcement and government requests for data should begin publishing annual transparency reports that elaborate on the requests received and the company response.

Companies can also consult the following resources for further guidance:

- i. The [GNI Principles on Freedom of Expression and Privacy](#) provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally.
- ii. The [Trusted Cloud Principles](#) establish key principles for cloud service providers committed to 1) safeguarding the privacy and security of their customers' data, and 2) working with governments to ensure the free flow of data, to promote public safety, and to privacy and data security in the cloud.

### **Industry Collaboration**

Collaborate with companies across the SaaS sector and the broader tech industry to better understand the human rights risks of SaaS products, platforms, and services; to share insights; and to establish overarching guidance and best practices.

### **Consider Creating a Multi-Stakeholder Initiative to Explore SaaS Sector Human Rights Impacts on an Ongoing Basis**

Engage with SaaS companies, expert stakeholders, and the broader tech industry to discuss common risks and explore the potential for consistent or collaborative approaches.

Engage with SaaS companies, expert stakeholders, and the broader tech industry to discuss common risks and explore the potential for consistent or collaborative approaches.

This could involve establishing a working group of SaaS companies and civil society organizations to focus on human rights due diligence of the SaaS Sector. This may include exploration of identified risks, emerging issues, human rights impact assessments of specific categories of products (similar to the HRIA of 5G), or guidance on stakeholder engagement, as well as issues beyond human rights, such as ESG issues or responding to investor and shareholder needs.

### **Consider Establishing an Independent Review Committee to Advise the SaaS Sector**

This committee would act as a review body for companies looking for guidance or feedback on specific human rights issues, or mechanisms through which they can engage relevant stakeholders and rightsholders. Examples of industry review committees include the

Independent Bioethics Advisory Committee (IBAC)<sup>32</sup> and the Ethical Review Process being designed by the Future of Privacy Forum (FPF)<sup>33</sup>.

### **Embed Human Rights into Business Strategy**

The SaaS sector is at the beginning of the human rights journey, and the actions above are key to implementing a human rights-based approach. As a long-term goal, we hope to see companies embed human rights into their overarching business strategies. This includes re-orienting sales goals to target the most socially beneficial, rights-respecting opportunities.

Companies can take a wide range of affirmative, positive, and proactive actions to advance the enjoyment of human rights.

When developing new services, solutions, and technologies, companies can support the realization and enjoyment of human rights by directly engaging rightsholders and intended beneficiaries, especially those most vulnerable, into their product design, development, and deployment processes, and by using the UN Sustainable Development Goals as an inspiration for innovation. This way, companies can deliberately seek to serve unmet needs through the intentional development of commercially viable, rights respecting, and inclusive business models that foster opportunity, expand access, and improve lives for everyone.

# VI. Annex

## Differentiating Characteristics

In the third section of this report, we outline eight characteristics of SaaS services related to their functionality and deployment, which may surface different human rights issues and provide different degrees of leverage to address them. Here, we provide additional detail on these characteristics.

### 1. Open versus closed platform

SaaS services fall into different categories on the spectrum of being open to or closed to user-generated content. While content sharing is the core service model of some SaaS services, those that provide technical infrastructure typically don't involve any content sharing.

CLOSED

#### Software closed to content sharing

- SaaS providers face fewer content-related issues.
- If the product or service allows for communication between users within the same company, there may still be a certain level of content-related issues.

#### Software open to content sharing

- There is increased risk of harmful user-generated content such as hate speech, violent or extremist content, harassment, or illegal activities.
- SaaS providers have more opportunities to proactively identify misuse on their platforms.
- SaaS providers need to consider deploying additional measures such as policies and resources for content moderation, which may lead to labor rights considerations in the value chain.

OPEN

## 2. Volume and sensitivity of data processed

SaaS services rely on data input on varying levels. The degree to which a service processes sensitive personal data may surface different kinds of human rights impacts.

NON-SENSITIVE

### Software using non-sensitive data

- Bias and discrimination can still occur, but in less visible ways. For example, if a factory operations software is designed for a certain market, it may not consider differences in the ways that factories operate in other geographies.
- Even if sensitive personal data is not used, algorithms may have unintended ripple effects on human rights. For example, using seemingly benign machine data, companies may make decisions about labor scheduling and worker conditions.

### Software using sensitive data

- The likelihood of human rights harm related to privacy and data governance rises as the volume and sensitivity of the data processed by the SaaS provider increases. Depending on where the data is stored, SaaS providers may be connected to potential human rights harms on various levels and may or may not have leverage to address them.
- If a SaaS service is inputting sensitive user data into AI models, the likelihood of human rights harm increases.

SENSITIVE

## 3. Level of automation involved

Some SaaS services incorporate machine learning and artificial intelligence systems to analyze data and generate insights. The degree to which a SaaS service involves automation may lead to different kinds of human rights impacts, or it may exacerbate the severity or likelihood of certain risks.

LESS AUTOMATED

### Software involving less automation

- There is increased risk of human error leading to human rights impacts.

### Software involving more automation

- When a SaaS service incorporates AI models and automation, the likelihood and severity of human rights risks may be higher.
- The use of AI may also lead to an increased number of errors going unnoticed, making human rights impacts less easily remediable.
- SaaS providers may be more directly linked to harms caused by flawed algorithms, but they may also have more leverage to remediate adverse impacts.

MORE AUTOMATED

## 4. Level of interoperability

The SaaS service model increases opportunities to integrate different software services. For some SaaS services, interoperability with other apps is an important feature that may surface new risks.

LESS INTEROPERABLE

### Less interoperable software

- SaaS providers may be more closely connected to potential human rights impacts and may have increased leverage to address them if their software is not integrated with others.

### More interoperable software

- If a SaaS service can easily be integrated with others, the combined use of these services may increase the likelihood of human rights impacts, and they may be less foreseeable by the SaaS provider.
- Interoperability reduces the technological barrier of integration for complicated software processes such as facial recognition. Consequently, it is easier for users to access or deploy capabilities such as surveillance activities, which can increase the likelihood of human rights violations.

MORE INTEROPERABLE

## 5. Cloud versus on-premises deployment

Although the definition of software-as-a-service suggests a cloud-based service model, some SaaS providers offer the option of deploying their software on-premises as well. Different issues surface and different amounts of leverage are needed to address them depending on whether a service is hosted on cloud or on-premises.

### Software deployed on-premises

- SaaS services deployed on-premises offer less visibility into customer use.
- In on-premises deployments, the customer is responsible for the management of the software, giving SaaS providers less leverage to address potential human rights impacts.
- On-premises deployment models typically lack the data security capabilities that are available in the cloud, making data breaches more likely and less foreseeable.

### Software deployed on the cloud

- SaaS services deployed on the cloud rather than on-premises are likely more easily integrated with other services, increasing the likelihood of risk.
- While cloud solutions generally employ sophisticated encryption and data protection measures, they also increase the number of actors with access to sensitive data. Data localization requirements around the world may put cloud-based SaaS providers into conflict with governments, especially in the case of privacy-violating information requests by authoritarian regimes.
- Cloud deployment models offer greater visibility into customer use; therefore, risks related to end-use are arguably more foreseeable in cloud deployments. This indicates that when software is deployed on the cloud, the provider is more closely connected to potential human rights impacts.
- In cloud deployments, SaaS providers are responsible for the management of the software, giving them greater leverage to address potential human rights impacts.

## 6. Sales model

SaaS providers employ a variety of sales models depending on the customer size, geography, and how much customization the product or service requires. A crucial differentiating factor for determining risk is the degree to which providers interface with their customers before and after sales.

LIGHT-TOUCH

### Software with light-touch sales model

- It is more difficult to integrate customer gating measures for products and services that are self-sign-up. Therefore, issues around objectionable customers, controversial use cases and new market entry are more prevalent.
- With off-the-shelf products and services, SaaS providers have less visibility into customer use, increasing the likelihood of product misuse and abuse.

### Software with high-touch sales model

- SaaS services with a high-touch sales model involve greater customer engagement, giving the SaaS provider more opportunity to undertake customer due diligence. This, in turn, decreases the likelihood of potential human rights harms related to customer end-use.
- With more customer engagement, SaaS providers have higher visibility into customer use cases, making it easier to anticipate potential harms.
- This would more closely connect SaaS providers to potential human rights impacts and give them more leverage to address them.

HIGH-TOUCH

## 7. Level of customizability

SaaS providers offer varying levels of customizability—some software is ready-made, whereas some allows the customer to change the code. The degree to which a SaaS service is customizable may have implications on the SaaS provider’s connection to harm.

NOT CUSTOMIZABLE

### Software that is not customizable by the customer

- SaaS services that are not customizable introduce fewer unanticipated use cases, decreasing the likelihood of human rights risks.

### Software that is highly customizable by the customer

- Highly customizable SaaS services are more likely to be connected to harm since customers can change the services’ functionality and outcomes, making potential harms less foreseeable by the SaaS provider.
- This may indicate that providers have less leverage to address potential impacts.
- On the flip side, if a SaaS service has been customized for the specific needs of a specific company, switching costs may increase, indicating increased leverage for the SaaS provider to address potential impacts.

HIGHLY CUSTOMIZABLE

## 8. Level of substitutability

Some SaaS services are more difficult to substitute than others due to their unique functionality, their “stickiness,” or switching costs. Typically, substitutability level correlates to the SaaS provider’s market power. The degree to which SaaS services are interchangeable may have implications on the SaaS provider’s leverage to address a potential human rights harm.

EASY TO SUBSTITUTE

### Software that is more easily substituted

- If a SaaS service is more easily substitutable, the service provider may have less leverage to do address potential human rights harms.

### Software that is less easily substituted

- If a SaaS service is less substitutable, the SaaS provider has higher leverage to address potential human rights harms associated with the use of their service.

DIFFICULT TO SUBSTITUTE

## Endnotes

- 1 [Gartner Says Four Trends Are Shaping the Future of Public Cloud](#), Gartner, 2021.
- 2 A series of UN B-Tech project papers have elaborated on the technology sector's responsibility to conduct downstream human rights due diligence (HRDD). Downstream HRDD will likely also be included as a requirement in the [forthcoming EU Mandatory Environmental and Human Rights Due Diligence Law](#).
- 3 See BSR's report [Human Rights Due Diligence of Products and Services: Assessing the Downstream Value Chain](#).
- 4 [Gartner Says Four Trends Are Shaping the Future of Public Cloud](#), Gartner, 2021.
- 5 See BSR's report [Responsible Product Use in the SaaS Sector](#).
- 6 [Leading software as a service \(SaaS\) countries worldwide in 2021, by number of companies](#), Statista, 2021.
- 7 A vast spectrum of SaaS services exists within each of these categories. The International Data Corporation (IDC) has developed a cross-cutting typology of 15 SaaS solutions based on the business needs they address; however, this categorization is not exhaustive and oversimplifies the complexity and range of SaaS service offerings.
- 8 See [Navigating the Tech Stack: When, Where and How Should We Moderate Content?](#) by Joan Donovan, and [A Framework for Moderation and Moderation in Infrastructure](#) by Ben Thompson.
- 9 [Parler claims it was also dropped by Slack after Amazon and other tech giants cut ties with the controversial social media company](#), Business Insider, 2021.
- 10 See BSR's report [Human Rights Assessments: Identifying Risks, Informing Strategy](#).
- 11 Ibid.
- 12 Ibid.
- 13 See BSR's [Human Rights Assessment: Identifying Risks, Informing Strategy](#), and [The Danish Institute of Human Rights \(DIHR\) human rights impact assessment guidance and toolbox](#), and [Oxfam community-based human rights impact assessment as examples](#).
- 14 See [Sector wide impact assessments \(SWIA\)](#) by the Danish Institute of Human Rights.
- 15 [Human Rights Due Diligence of Products and Services: Assessing the Downstream Value Chain](#), BSR, 2021.
- 16 See [Seven Questions to Determine a Company's Connections to Human Rights Abuses](#) by Jonathan Drimmer and Peter Nestor for guidance on how to use the cause/contribute/directly linked framework.
- 17 [The B-Tech Project](#) aims to translate the UN Guiding Principles on Business and Human Rights (UNGPs) to the technology sector. It is an initiative of the Office of the United Nations High Commissioner for Human Rights.
- 18 See the B-Tech Foundational Paper [Taking Action to Address Human Rights Risks Related to End-Use](#).
- 19 [Human Rights Due Diligence of Products and Services: Assessing the Downstream Value Chain](#), BSR, 2021.
- 20 [UN Guiding Principles on Business and Human Rights](#).
- 21 See BSR's report [Human Rights Due Diligence of Products and Services: Assessing the Downstream Value Chain](#).
- 22 See [With Great \(Computing\) Power Comes Great \(Human Rights\) Responsibility: Cloud Computing and Human Rights](#) by Vivek Krishnamurthy.
- 23 See [Section 3](#) of this report for a more detailed description of the differentiating characteristics.
- 24 See the B-Tech Foundational Paper [Addressing Business Model Related Risks](#).
- 25 See BSR's report [The Shared Opportunity to Promote: A Second-Decade Priority for the UNGPs](#).
- 26 See [With Great \(Computing\) Power Comes Great \(Human Rights\) Responsibility: Cloud Computing and Human Rights](#) by Vivek Krishnamurthy.
- 27 See Principle 19 of the [UN Guiding Principles on Business and Human Rights](#) for a more detailed description.
- 28 See [Responsible Use of Technology](#) by BSR and WEF.
- 29 See BSR's report [Responsible Product Use in the SaaS Sector](#) for further guidance on standard components to include in an Acceptable Use Policy.
- 30 There are a wide range of available indices spanning specific human rights issue areas; however, those most relevant to SaaS companies in high-risk areas pertain to (i) the presence of armed international or non-international conflict or military occupation (see [RULAC](#)) (ii) the incidence of ongoing mass violence (see [Global Peace Index](#), [ACLED](#), [V-Dem Physical Violence Index](#)) (iii) the rule of law ([World Justice Project](#), [Global State of Democracy Index](#)), (iv) discrimination ([V-Dem Social Group Equality In Respect For Civil Liberties Indicator](#)) and (v) freedom online ([Freedom House's Freedom on the Net Score](#)).
- 31 H&M and Microsoft have both piloted such programs. H&M hosts an [Ethical AI Debate Club](#) to discuss fictional scenarios and ethical dilemmas related to the use of AI in the fashion industry. Microsoft has established a "champs" program that designates resident experts who raise awareness and provide advice and assistance on ethical and human rights issues related to AI.
- 32 [Independent Bioethics Advisory Committee \(IBAC\)](#).
- 33 [Ethical Review Process](#) being designed by the Future of Privacy Forum.

The conclusions presented in this document represent BSR's best professional judgment, based upon the information available and conditions existing as of the date of the review. In performing its assignment, BSR relies upon publicly available information, information provided by member company, and information provided by third parties. Accordingly, the conclusions in this document are valid only to the extent that the information provided or available to BSR was accurate and complete, and the strength and accuracy of the conclusions may be impacted by facts, data, and context to which BSR was not privy. As such, the facts or conclusions referenced in this document should not be considered an audit, certification, or any form of qualification. This document does not constitute and cannot be relied upon as legal advice of any sort and cannot be considered an exhaustive review of legal or regulatory compliance. BSR makes no representations or warranties, express or implied, about the business or its operations. BSR maintains a policy of not acting as a representative of its membership, nor does it endorse specific policies or standards. The views expressed in this document do not reflect those of BSR member companies. The conclusions presented in this document represent BSR's best professional judgment, based upon the information available and conditions existing as of the date of the review. In performing its assignment, BSR relies upon publicly available information, information provided by member company, and information provided by third parties. Accordingly, the conclusions in this document are valid only to the extent that the information provided or available to BSR was accurate and complete, and the strength and accuracy of the conclusions may be impacted by facts, data, and context to which BSR was not privy. As such, the facts or conclusions referenced in this document should not be considered an audit, certification, or any form of qualification. This document does not constitute and cannot be relied upon as legal advice of any sort and cannot be considered an exhaustive review of legal or regulatory compliance. BSR makes no representations or warranties, express or implied, about the business or its operations. BSR maintains a policy of not acting as a representative of its membership, nor does it endorse specific policies or standards. The views expressed in this document do not reflect those of BSR member companies.



BSR™ is an organization of sustainable business experts that works with its global network of the world's leading companies to build a just and sustainable world. With offices in Asia, Europe, and North America, BSR™ provides insight, advice, and collaborative initiatives to help you see a changing world more clearly, create long-term business value, and scale impact.

**[www.bsr.org](http://www.bsr.org)**

Copyright © 2022 by Business for Social Responsibility (BSR)

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.