HOW TO RESPECT PRIVACY AND FREE EXPRESSION AS A TECH SME IN MALAWI

GLOBAL PARTNERS DIGITAL

Acknowledgements

This guide was written by Charles Bradley, Richard Wingfield, Jonathan Jacobs and Sebastian Smart.

With special thanks to Michael Samway, Nicole Karlebach, David Sullivan, Rebecca MacKinnon, Vivek Krishnamurthy and Fadzai Madzingira.

Design by Jon Parkinson.

The development of this guide was made possible with support from Facebook.


GLOBAL
PARTNERS
DIGITAL

Contents

Foreword

The privacy, security, and free expression of users should be fundamental considerations for any business operating in Malawi – especially in the tech sector.

For one thing, these rights are protected by international, regional and Malawian human rights law. But that isn't the only reason. In fact, there's a very strong business case for respecting them.

Unfortunately, this message hasn't been cutting through. Many businesses remain in the dark about the advantages of respecting privacy and free expression, and the risks if they don't.

This guide, developed by Global Partners Digital, aims to remedy this.

HOW DO I USE THE GUIDE?

In **Section 1**, we set out the business case, looking at the three key reasons why businesses benefit from respecting privacy and free expression.

In **Section 2**, we examine what privacy and free expression actually mean, and how they might arise as issues for tech businesses to consider.

In **Section 3**, we look at the obligations businesses have to respect human rights.

Section 4 is about putting these lessons into action; with a three-stage guide to making your business human rights-respecting.

In **Section 5**, we show businesses how to act in specific scenarios where their policies on privacy and free expression are tested.

And we conclude with a list of **Useful resources**.

WHO IS THIS GUIDE FOR?

The guide was developed for people working in senior positions at tech SMEs (for example, CEO, COO or Legal Counsel). However, it may also be useful for other members of staff as well as civil society organisations and consumer groups who have an interest in these issues.

The full benefits of this guide will be gained by reading it in its entirety, however, **Section 4** sets out possible courses of action to take and can be used as a standalone resource.

01

Why should I respect privacy and free expression?

“[I]f a business properly respects human rights, then in all likelihood it will be more profitable. [...] Studies show that where there is greater engagement, this leads to increased trust, which in turn leads to enhanced profitability.”

Richard Karmel
Partner at Mazars

The title of this guide is “How to respect privacy and free expression as a tech SME in Malawi”.

But if you work for a tech SME, you might wonder why you even need to think about these issues. “Aren’t they problems for human rights defenders?”, you might ask. “My focus is on building innovative products for my users”.

One of our biggest aims in this guide is to change these perceptions. In fact, there’s an excellent business case for respecting the privacy and free expression of your users – especially if you are a tech SME. Doing so can not only help you avoid reputational risks and legal problems. It can also have an actively positive effect on your business – making it more competitive, more sustainable, and, ultimately, more profitable.

Not convinced? Here are **three reasons** why respecting privacy and free expression is good for your business.

Your users will have more trust and confidence in your products and services

Consumer trust is make or break for any business – but it's especially crucial in the tech sector. After all, if you are selling a digital product, service, app, or solution, you will likely be asking your customers to share a lot of sensitive data about themselves. To do this, they need to know that they can trust you to handle that data.

But customers around the world are becoming less trusting. At the same time, trends show that they are increasingly concerned about their privacy and free expression, and are making purchasing decisions based on how far companies go to respect these rights.

It's not difficult to understand why. Imagine I'm the customer of a messaging app, for example, and I find out that the company that makes the app has been handing data on its users to governments. Am I likely to continue using that app, or switch to an alternative?

59%

of US consumers surveyed said they'd be less likely to buy from a company if they knew it had suffered a data breach.

(Deloitte, 2015)

Similarly, if a company I have bought a product from suffers a data breach – exposing my address, date of birth, and personal banking details – what is my response likely to be?

That's what happens when you lose consumer trust through bad privacy and free expression practices.

But if you win their trust?

Big opportunities. Because once people know your company has great data protection and privacy policies, uses encryption, and refuses to share their data with the government, they might be more likely to use your products, and stay with them. You may even find yourself taking customers away from competitors who have a weaker record on these rights. ProtonMail, a Swiss email service with end-to-end encryption and excellent privacy policies, is a good example of a company that turns respect for human rights into a competitive advantage.

So, to sum up: respecting privacy and free expression means more consumer trust, more customers, and better retention. Sound good? In **Section 4**, we'll outline some practical ways you can start benefiting from this equation.

You'll get more investment and opportunities for growth

Investment is essential to the growth of any business. But investors – whether based in Malawi or overseas – are demanding, discerning, and easily scared away. After all, they want to know that you are reliable, trustworthy, and that you'll give them a good return on their investment.

So what kinds of things will they be looking for? **User trust and confidence** (which we talked about above) is a big factor, and **legal compliance** (which we'll talk about next) is also critical. Again, this is just common sense – investors don't want to put their money into a business which has a bad reputation, or is dogged by legal issues. **A good record on privacy and free expression** is a great way to show them that you are a safe pair of hands.

At the same time, **ethical considerations** – including respect for human rights like privacy and free expression – are becoming a serious factor for many investors, especially those in institutions like Bloomberg or Morgan Stanley, which are expanding their **environmental, social, and governance** service offerings for major financial firms. In the last five years, the value of socially responsible funds globally has risen by **76%** to over $200 billion.

Want to attract some of that? In **Section 4**, we outline some simple steps you can take to show investors you're an ethical, responsible destination for their capital.

> **"As investors we believe that establishing the respective obligations of States and businesses will enhance the operating environment for companies in which we invest and their long term prospects for financial success."**
>
> From the Investor Statement in support of the Guiding Principles on Business and Human Rights, signed by 87 investors representing $5.3 billion

You have to — because of the law!

An obvious but important reason. As a business in Malawi, you have a legal responsibility to respect the human rights of your users.

Article 15(1): The human rights and freedoms enshrined in this Chapter shall be respected and upheld by the executive, legislature, judiciary and all organs of the Government and its agencies and, where applicable to them, by all natural and legal persons in Malawi and shall be enforceable in the manner prescribed in this Chapter.

Constitution of Malawi

We'll go into this in more detail in **Section 3**, but the human rights obligations in Malawi's Constitution are binding not only on the government and other state agencies, but "all natural and legal persons" – which includes businesses.

No business wants to have to go to court – and it can easily happen, especially to a tech SME. A data breach caused by inadequate security could open you up to a huge number of lawsuits.

The best way to prevent this happening? Make sure your business has **policies which respect the privacy and free expression of your users.** As we've discussed above, this will have the added advantage of improving your **brand reputation** and **user trust**, and encouraging investment.

We explain how you can do all this in **Section 4**. But before that, let's take a closer look at what these terms – privacy and free expression – actually mean.

02

What are privacy and free expression?

So now we've seen why respecting privacy and free expression can be positive for your business (and why failing to respect them can harm it).

In this section, we're going to take a closer look at what privacy and free expression mean in legal terms, and what your responsibilities are as a business – both in Malawi, and at the international level. Then, we'll look at two (hypothetical) examples of how a tech SME might find itself in breach of these obligations.

Privacy

Privacy, in human rights terms, refers to your right to create a sphere of privacy around yourself, free from interference by the government or others.

Among other things, this also covers your ability to:

- communicate with others privately, free from surveillance, interception, or other interference;
- decide how you want to exercise your autonomy; for example, by choosing who you want to form relationships and friendships with.

The scope of privacy also includes includes aspects of security, including:

- the protection and confidentiality of personal information and data;
- the ability to access information and data which has been retained about you; and
- the ability to have incorrect information held on you corrected or deleted.

Privacy is a fundamental human right and is binding in Malawi both as a matter of international law and national law through the Bill of Rights in the Constitution.

Malawi's Constitution protects the right to privacy as follows:

Every person shall have the right to personal privacy, which shall include the right not to be subject to: (a) searches of his or her person, home or property; (b) the seizure of private possessions; or (c) interference with private communications, including mail and all forms of telecommunications. (Article 21)

The right to privacy is not, of course, absolute. But it can only be limited or restricted in circumstances when:

- there is a clear legal basis;
- it is necessary to meet an objectively pressing need such as to prevent crime; and
- it is a proportionate response to that need.

As a tech SME, a lot of your everyday actions and practices have implications for the right to privacy. For example:

- any collection of personal information or data by a public body or business (including information about their identity, contact details, location, activities, financial information and health);
- the use, processing and disclosure of that data;
- any breaches or hacks of that data;
- sharing of private communications and information; and
- surveillance of individuals.

Free expression

In the international human rights framework, freedom of expression refers to the right to be able to freely express yourself and to seek and receive information, ideas, and the expression of other people.

Like privacy, it is a fundamental human right, and is binding in Malawi through the Declaration of Rights in the Constitution:

Every person shall have the right to freedom of expression. (Article 35.)

Freedom of expression is typically understood as covering two dimensions: content (modes of expression) and form (means of expression).

Let's look at **content** first. As well as covering everyday, basic modes of communication – for example, chatting to a friend about the weather – the right to freedom of expression also covers:

- journalism;
- political discussions;
- discussion of human rights;
- cultural and artistic expression;
- religious discussions; and
- teaching.

Freedom of expression also covers all **forms** of expression and communication. That includes:

- speech;
- letters and printed media;
- email;
- text messaging;
- social media; and
- instant messaging.

And free expression does not only cover "appropriate" or "acceptable" expression. It also covers expression which offends, shocks or disturbs.

As a tech SME, your everyday actions and practices can have implications for the right to freedom of expression. Here's a few examples of protected content and forms of expression you might host or handle:

- posts and messages on social media;
- blog posts;
- news articles and comments on websites;
- discussions on online forums;
- private communications through email, text messaging, social media, and instant messaging;
- online cultural and artistic expression; and
- online education and teaching.

As with the right to privacy, restrictions on freedom of expression, such as through censorship or surveillance, are only permitted in very limited circumstances when:

- there is a clear legal basis
- it is necessary to meet an objectively pressing need, such as to prevent crime; and
- it is a proportionate response to that need.

03

What are my legal obligations as a business regarding privacy and free expression?

In this section, we're going to take a closer look at what your legal responsibilities in relation to human rights are as a business, looking both at international standards and national law. Then, we'll look at two (hypothetical) examples of how a tech SME might find itself in breach of these obligations.

UN Guiding Principles on Business and Human Rights

When it comes to international standards, the United Nations **Guiding Principles on Business and Human Rights** is the crucial document.

Developed and unanimously endorsed by the 47 states in the UN Human Rights Council, these principles set out the role that states and businesses should have in respecting human rights – known as the "Protect, Respect and Remedy" framework.

While not legally binding, they constitute what is called "soft law", which means that they set out the current understanding of the requirements of international law relating to business and human rights. As such, they may have a significant influence on governments and courts when they are making and interpreting law.

This "Protect, Respect and Remedy" framework also sets out how states and businesses should engage with each other on human rights and mutually reinforce each other's responsibilities:

- The state's role is to **implement a legislative and policy framework** that makes sure human rights are respected by businesses.
- The role of businesses is to **urge governments to fulfil their obligations under the Guiding Principles** – for example, by advocating for the amendment of laws and policies that put human rights at risk.

That's all quite useful as a broad definition of the obligations businesses have in respecting human rights. But it doesn't tell us much about how these obligations might apply in specific contexts. After all, there are a lot of human rights, and a lot of different business sectors. A multinational mining company and a tech SME based in Malawi are likely to fulfil their human rights obligations in very different ways.

UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS

PROTECT	RESPECT	REMEDY
Sets out the responsibilities of **governments.**	Sets out the responsibilities of **businesses.**	Sets out the responsibilities of both **governments** and **businesses.**
Focuses on ensuring that there are appropriate laws, regulations, and policies in place so that businesses respect human rights.	Focuses on ensuring that businesses respect human rights in practice.	Focuses on the need for both governments and businesses to ensure that there are appropriate processes and remedies in place for when human rights are violated by businesses.

THE KEY PRINCIPLES TO KNOW

- ***Principle 11*** *says business enterprises should respect human rights.*
- ***Principle 13*** *says businesses should: (a) avoid causing or contributing to negative human rights impacts through their activities and address such impacts where they occur, and (b) take steps to prevent or mitigate negative human rights impacts which are directly linked to their operations, products, and services.*
- ***Principle 14*** *says that this obligation applies to businesses of all sizes, sectors, operational contexts, ownership models, and structures (although the way businesses have to meet this obligation varies depending on these factors).*
- ***Principle 15*** *says that businesses should put in place policies and processes appropriate to ensuring respect for human rights, such as a policy commitment, a human rights due diligence process, and remedial processes where negative human rights impacts occur.*

GNI Principles on Freedom of Expression and Privacy

Luckily for us, the **Global Network Initiative** – a multistakeholder coalition of businesses, civil society organisations, investors, and academics – has developed the **GNI Principles on Freedom of Expression and Privacy**, which specifies how tech businesses should respect the rights to freedom of expression and privacy.

They are as follows:

PRIVACY

- *Participating companies will **employ protections with respect to personal information** in all countries where they operate in order to work to protect the privacy rights of users.*
- *Participating companies will **respect and work to protect the privacy rights of users when confronted with government demands, laws, or regulations that compromise privacy** in a manner inconsistent with internationally recognized laws and standards.*

FREEDOM OF EXPRESSION

- *Participating companies will respect and work to protect the freedom of expression of their users by **seeking to avoid or minimize the impact of government restrictions on freedom of expression**, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.*
- *Participating companies will respect and work to protect the freedom of expression rights of users **when confronted with government demands, laws, and regulations to suppress freedom of expression**, remove content or otherwise limit access to communications, ideas and information in a manner inconsistent with internationally recognized laws and standards.*

National laws

As well as these international standards, there is also national law which businesses need to comply with.

We have looked at the most relevant provisions of Malawi's Constitution protecting human rights in **Section 2**, and Article 15(1) of the Constitution explicitly states that the human rights and freedoms enshrined in it must be respected and upheld by "all natural and legal persons", which includes businesses. As well as this constitutional protection for human rights, there are also specific laws which protect aspects of the right to privacy, particularly the Electronic Transactions and Cyber Security Act, 2016, which places explicit obligations on businesses. These obligations can be summarised as follows:

- Data controllers must ensure that personal data is processed fairly and legally; collected for specific, explicit and legitimate purposes and used for such purposes only; adequate, relevant and not excessive in relation to the purposes for its collection and use; accurate and kept up to date; and kept in a form which enables identification of the data subjects for no longer than is necessary for the purposes for which the data has been collected and processed.
- Personal data can only be processed for the following reasons: if the data subjects has unambiguously given consent; if it is necessary for performance of a contract; if it is necessary to comply with a legal obligation; if it is necessary to protect the data subject's vital interest; if it is necessary for the performance of a task carried out in the public interest; or if it is necessary for the purposes of the data controller's legitimate interests (but only where these interests are not overridden by the data subjects' human rights).
- Data subjects have the right to obtain confirmation on whether their data is held and, if so, what data is held and for what purpose. Data subjects can object at any time to the processing of their personal data and, if that objection is justifiable, the data controller may no longer process that data. Data subjects also have the right to have data rectified, erased, or blocked where the provisions of the law have not been complied with.
- Data controllers must implement technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and all other unlawful forms of processing.

Real life scenarios

Maybe all this still seems quite abstract and removed from your situation. After all, we're talking about very serious things here: violations of privacy and freedom of expression. *Fundamental human rights*. Surely this only applies to tech giants – not a small business?

In fact, violations can happen easily in the tech sector, regardless of the size of your company. Take a look at the below scenarios to see how.

How a tech SME could violate privacy

A company keeps all its user data in a single database accessible to all staff. This data includes contact details, such as addresses, telephone numbers, and email addresses. A junior member of staff uses the database to find the telephone numbers and email addresses of young women and contacts them by telephone and email, asking to meet with them, and threatening abuse if they refuse.

This is a violation of the right to privacy for several reasons:

- Unwanted calls and threats from another individual represents a breach of private space and thus of the person's privacy.
- The protection and confidentiality of personal information and data has been violated.
- As a restriction on privacy, this is neither necessary to meet an objectively pressing need such as to prevent crime, nor a proportionate response to that need. Here there is no legal basis for the actions of the member of staff and it is not necessary to meet any objectively pressing need.

How a tech SME could violate free expression

A small tech company hosts a website which enables users to publish opinion pieces and articles about politics. Some readers and representatives of the police contact the company, asking for an article about a particular politician to be taken down from the website on the grounds that it is "unfair", "offensive", and "stirring up trouble". The company decides to take the article down to avoid further controversy.

This would be a violation of the right to freedom of expression because:

- Free expression includes receiving and imparting information and ideas, including on political and public affairs. It includes all forms of information and ideas, even those which are controversial or offensive. Online, as well as offline, expression is covered. The website's articles and comments are thus protected under the right to freedom of expression.
- Restrictions are only permissible if (i) there is a clear legal basis, (ii) it is necessary to meet an objectively pressing need, and (iii) if it is proportionate. First of all, there is no clear legal basis for this restriction and no-one has set out which law prohibits "stirring up trouble". Second, avoiding offence or debate of controversial issues is not an objectively pressing need for limiting freedom of expression. There is no evidence of any risk of crime or disorder because of the articles or comments.

04

How can I make sure I respect these rights?

So far, we've looked at why respecting privacy and free expression can be good for your business (Section 1); what these rights mean (Section 2); and what your specific obligations are as a tech SME (Section 3).

Now it's time to see how you can start putting these lessons into practice.

In this section, you'll find a **three stage programme**, designed specifically to help your business attain best practice status on privacy and free expression. Don't worry about trying to tackle everything at once. As you go through the programme, you'll get a better picture of what actions are relevant and feasible for your business to take.

You may find that this programme throws up more questions than answers, but that's not necessarily a bad thing. There's no one size fits all approach and you shouldn't be afraid to experiment, once you've understood the basics.

And at the end of the guide, we've created a list of **Useful resources** that will help you develop and push yourself further.

Stage 1: Review your practices

The first (and easiest) stage is to conduct a simple review of your company's policies, products, and services to identify where privacy, security and free expression issues might arise, or where they might be at risk.

This will help you start to see where you can avoid risks and take advantage of new opportunities, and will set you up for the next stages, which are focused on **consolidating your understanding** and **taking action.**

In this stage, we've outlined a list of questions which will help you assess the potential impacts of your business practices on **privacy and security** and **free expression**. By working through them, you should end up with:

- A better picture of your business's current performance on privacy, security, and free expression;
- An early idea of where you might start improving and developing your practices.

Privacy, security, and free expression review: questions to ask

PRIVACY AND SECURITY

Does your business collect any information or data relating to or generated by users? If it does:

What kind of information or data does it collect? For example:

- Personal details (name, address, contact details);
- Location data (through the use of GPS or otherwise);
- Communications data (including both the content of communications and communications metadata, e.g. when communications were made, and to whom);
- Financial information (bank details and details of transactions made); and
- Health information.

How is that information or data stored?

What steps are being taken to ensure the security of that information or data?

Are there systems in place to limit and monitor employee access to user information and data?

Are users informed that this information or data is collected? And what steps are in place to make sure their consent is obtained?

Is there a way for users to find out what information or data has been collected?

Is there a way for users to request that any information or data relating to them is permanently deleted?

Does your business ever disclose information or data relating to its users to third parties? If it does:

- What information or data is disclosed and for what purposes?
- Are users informed of this disclosure and what steps are in place to make sure their consent is obtained?

Does your business ever receive requests for information or data from the government, the police or security services, or any other public bodies? If it does:

- What information or data is requested and for what purposes?
- What policies or processes are in place to decide whether such requests are granted?

FREE EXPRESSION

Does your business's services or products allow for individuals to create content or express themselves, whether publicly or privately? This could include, for example:

- The ability for users to publish videos, audio files, articles, or posts;
- The ability for users to respond to existing content via comments or otherwise;
- The ability for users to use online forums for discussion;
- The ability for users to communicate with others, whether publicly or privately.

Does your business have any policies or rules on unacceptable content or content which will be removed? If so:

- Are they in line with the acceptable limitations on free expression?
- Are these policies or rules publicly accessible?

Does your business ever receive requests for the deletion, removal or restriction of content or expression? If it does:

- Who are these requests received from?
- What policies or processes are in place to decide whether such requests are granted?
- Are the individuals concerned informed of these requests?

Stage 2: Consolidate your understanding

Once you've completed Stage 1, you should have a better idea of the aspects of your policies, products, and services which might have a negative impact on privacy and free expression.

The next step is to deepen what you've already learned and ensure that these learnings become rooted in your business. Here's some easy ways to start doing this:

Take some time to look at the resources highlighted in the Useful resources section of this guide (pp. 42–43) to get a better understanding of the role businesses should play in respecting privacy, security and free expression. In particular, you may want to look at

- The **UN Guiding Principles on Business and Human Rights**; and
- The Global Network Initiative's **Principles on Freedom of Expression and Privacy**.

Start conversations with other stakeholder groups – like civil society organisations and consumer groups – to find out what kinds of privacy and freedom of expression issues they are currently working on. You could also ask these groups to review your policies, products, and services, and tell you what they think the risks are. Getting an informed outside perspective can help you see problems you might have missed.

Develop and support internal learning opportunities, including at board level, to better understand privacy, security, and free expression, and share this learning more widely throughout the business.

Stage 3: Take action

You've reached the final stage. By now, you and your business should feel confident enough to start articulating your policies as they relate to privacy, security and free expression, and to think about what steps can be taken to avoid or mitigate negative impacts.

Below are some actions you can take to improve your business's approach to privacy and free expression. Links to the resources mentioned are in the **Useful resources** section (see **pp. 42–43**).

Develop a publicly accessible statement (or policy) on your business's commitment to respecting privacy, security, and free expression. For inspiration, take a look at AT&T's **Human Rights in Communication Policy**, Vodafone's **Privacy and security – Our approach**, and other examples on the Business & Human Rights Centre's resource page (**pp. 42–43**).

Develop a publicly accessible Privacy Policy or Content Policy, setting out specific answers to the questions in Stage 1. The AT&T and Vodafone documents mentioned above are good examples.

Develop a publicly accessible Action Plan, identifying areas where privacy and free expression are at risk, and what needs to happen to mitigate those risks.

Undertake publicly accessible Impact Assessments for any new products or services, to ensure risks to privacy and free expression are accounted for. For more guidance on Impact Assessments, access the **Business & Human Rights Centre's resource page**.

If you identify that your business has caused or contributed to a negative impact on privacy, security, or free expression, **ensure that a remedy is provided to the victim(s) through a clear process**.

Does your SME receive user data or content removal requests from governments or law enforcement agencies? If so, here are some further actions you might consider:

- **Scrutinise all requests to determine whether they are in accordance with international and national law** (i.e. is there a clear legal basis? is there a pressing need, e.g to prevent crime? is it proportionate?). If not, seek clarification from the actor making the request, and ask for written communication of the legal basis for the request and the name, title, and signature of the authorising official.
- **Publish information on** the number and type of requests received. See Google and Yahoo's transparency reports as examples (**pp. 42–43**).

05

What should I do if...?

Following the three stage programme outlined in the previous section will help your business respect privacy and free expression, reduce risks, and reap a range of benefits.

But this takes time. What if something happens that takes you by surprise? Like a sudden content request by a government, or a massive data breach.

Next, we've set out a list of three possible scenarios which might occur with guidance on how to respond in a way which respects privacy and free expression.

The police ask me for location data on a user?

Your company runs a mobile application which collects data generated by its users' mobile phones. One day you receive a request from the Malawian Police for the location and conversations of a specific user. The request contains minimal detail and simply says that the data is need for reasons of "national security".

Providing this user data could result in a serious breach of the user's privacy (as well as significant risks for your brand reputation).

To avoid this, these are the questions you should immediately ask:

- Is there an appropriate warrant or court order for the disclosure of the data, which includes the name, title, and signature of the authorising official? If not, you should request one and withhold the data until it is produced.
- If there is an appropriate warrant or court order, is the user aware that their data has been requested and is going to be disclosed? If not, you should, unless prohibited by the warrant or court order, inform the user of the request and any data that has been disclosed.
- Does your business have a publicly accessible policy on responding to requests for user data, which sets out the circumstances in which data will be withheld or disclosed? If not, your business should develop and publish such a policy.
- Does your business publish a transparency report on the number and type of requests received? If not, it should start publishing such reports.

My business suffers a data breach?

Your business is a mobile application which allows its users to pay for different services using mobile money. The app collects financial data from its users including bank details, a history of the financial transactions, and a log of where and when the app has been used. This data is not securely stored – and, following a hack, the bank details and geolocational data of thousands of your users is stolen. Some suffer financial loss as a result.

In the first instance, you should ensure a remedy is provided to the victim(s) through a clear process. The type of remedy you would provide would depend on a range of factors, including the nature and severity of the breach.

To minimise the risk of further harmful breaches in the future, here are some of the questions your business should immediately ask itself:

- How is my user information or data stored?
- What steps are being taken to ensure the security of that information or data?
- Are users being informed that this information or data is collected and what steps are in place to make sure their consent is obtained?
- Is there a way for users to find out what information or data has been collected?
- Is there a way for users to request that any information or data relating to them is permanently deleted?

I'm asked to censor "hate speech"?

Your company runs an online newspaper, which has published a number of articles about a particular political party ahead of an election. Your newspaper also has a function allowing readers to add comments to news stories. Some of the articles cover alleged misconduct and corruption, and many of the comments are critical of politicians and political parties. The online newspaper receives complaints from the politicians concerned, and some members of the public, demanding that the articles and comments be deleted as they are forms of "hate speech".

These are the questions you need to ask:

- Where is the request coming from? Is it from an individual member of the public, a person who is directly referred to in the content, or a law enforcement agency?
- Is there a clear legal basis for the article or comment to be removed? If not, the business should ask for the precise legal basis on which the article or comment is prohibited before considering any further action.
- Does the challenged article or comment actually amount to "hate speech" (as defined above) or some other form of prohibited speech (such as defamation)?
- Does your business have a publicly accessible policy on responding to requests for removal of articles or comments? If not, it should develop and publish such a policy.
- Does your business publish a transparency report on the number and type of requests for removal of article or comments received? If not, it should start publishing such reports.

Useful resources

CONTACTS

Global Partners Digital
www.gp-digital.org
info@gp-digital.org

Malawi Human Rights Commission
www.facebook.com/
HumanRightsCommissionofMalawi/
info@malawihrc.org

Business & Human Rights Support Centre
www.business-humanrights.org
contact@business-humanrights.org

Global Network Initiative
www.globalnetworkinitiative.org

FURTHER RESOURCES AND READING

Section 1: Why should I respect privacy and free expression?

Allison-Hope, D., 'Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry', Business for Social Responsibility (February 2011), available at: www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

Conroy, P., Narula, A., Milano, F. and Singhal, R., 'Building consumer trust: Protecting personal data in the consumer product industry', Deloitte (November 2014), available at: dupress.deloitte.com/dup-us-en/topics/risk-management/consumer-data-privacy-strategies.html

Edelman, 2017 Edelman Trust Barometer (2017), available at: www.edelman.com/trust2017

Karmel, R., 'Building respect for human rights and business through regulation', Business in the Community, (March 2015), available at: www.bitc.org.uk/blog/post/building-respect-human-rights-and-business-through-regulation

Schoemaker, D., "Raising the Bar on Human Rights:

What the Ruggie Principles Mean for Responsible Investors", Sustainalytics (August 2011), available at: www.sustainalytics.com/sites/default/files/ruggie_principles_and_human_rights_0.pdf

Section 2: What are my legal obligations as a business?

UN Guiding Principles on Business and Human Rights, available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

UN Guiding Principles Reporting Framework, available at: www.ungpreporting.org

Human Rights Commission and Danish Institute for Business and Human Rights (2015), Human Rights and Business country guide: Malawi, available at: https://globalnaps.org/wp-content/uploads/2018/04/business-and-human-rights-guide-to-malawi.pdf

Section 4: How can I make sure I respect these rights?

Global Network Initiative, 'Principles on Freedom of Expression and Privacy', available at: globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf and the Implementation Guidelines, available at: globalnetworkinitiative.org/sites/default/files/Implementation-Guidelines-for-the-GNI-Principles.pdf

Business & Human Rights Support Centre, available at: www.business-humanrights.org. See, in particular, its pages on:

Kenya: https://business-humanrights.org/en/regions-countries/africa/kenya

Technology, telecoms and internet: https://business-humanrights.org/en/tools-guidance-0/sector-specific-guidance/technology-telecoms-internet

AT & T', 'Human Rights in Communication Policy' available at: www.att.com/Common/about_us/downloads/Human_Rights_Communications_Policy.pdf

Vodafone, 'Privacy and security – Our approach', available at: http://www.vodafone.com/content/dam/sustainability/2015/pdf/operating-responsibly/privacy-and-security.pdf

GLOBAL
PARTNERS
DIGITAL

GLOBAL PARTNERS DIGITAL

SECOND HOME, 68 HANBURY STREET, LONDON, E1 5JL
+44 203 818 3258
INFO@GP-DIGITAL.ORG