Data privacy and protection

We are committed to ensuring data privacy and protection. This is core to our business.

Our commitment

We recognise that privacy is an important value and an essential element of public trust.

We strive to be a trusted company and we expect the same of all our businesses. We expect each business to implement responsible data-privacy practices in a way that is adapted to its own circumstances, which considers its business model, the cultures of the countries in which it operates, its compliance obligations, and its human and financial resources.

For many years we have viewed data privacy as critical for the group, not only in terms of good governance and risk management, but also to do the right thing and build trust with our key stakeholders. Accordingly, we have a comprehensive data-privacy governance policy and a privacy programme designed to ensure the vast amount of data across the different businesses within the group is protected and managed.

Our approach

A groupwide policy

Our policy on data-privacy governance sets out the responsibilities, principles and programmes for ensuring data privacy across the group.

It is designed to define and document how data privacy is managed in the group; to promote best practice; to accommodate the different business models, resources, culture and legal requirements across the group; and to support trust in our businesses' products and services.

Clear accountability

The critical foundation is to give clear accountability to individual businesses. Each business is directly responsible for managing data privacy in its organisation.

This responsibility rests ultimately with the CEOs of each business – they lead in implementing the group's policy and are directly accountable for the data-protection programmes and privacy standards in their organisations.

This approach to data privacy aligns with our model of decentralised governance and broader belief in encouraging great leaders and businesses to excel. We believe setting the right shared principles and giving businesses the direct responsibility to enact them is the best way to have a greater long-term positive impact. More broadly, we are fostering a culture of data privacy and looking to businesses to ensure privacy by design, where privacy becomes part of the fabric of day-to-day work rather than an add-on.

Seven data-privacy principles

Each business is expected to respect and implement seven core data-privacy principles. Widely recognised internationally as fair information privacy principles, they are ethical guidelines for the responsible use of data. Critically, they are both universal and able to be applied to the different businesses in the group – from established global players to start-ups in jurisdictions that may not yet have a data-privacy law.

Data-privacy programme

To help businesses put the principles into practice, we have a data-privacy programme designed to scale to their different needs and circumstances. This ensures that our core data-privacy commitment and approach is followed in ways that really work for our businesses. The programme has seven key elements: ensuring executive buy-in; knowing your data; setting policies; training employees; managing vendors and third parties; legal compliance; and reporting.

We are investigating the performance indicators that are most relevant for our operations to report on to our stakeholders.

Supporting and monitoring

The group's data-privacy office supports and monitors the businesses. Help ranges from guidance on implementing the data-privacy programme, a secondment programme that develops and trains future privacy leaders nominated by companies within the group, and advice on any data-privacy implications of mergers and acquisitions.

Businesses provide regular privacy and security reports to group executives as an integral part of ongoing business reviews. The board's risk committee reviews the data-privacy policy and its implementation annually as part of its oversight and governance responsibilities.

Our seven data-privacy principles:

1. **Notice.** We offer appropriate notice about our data-privacy practices.
2. **Individual control.** We honour data subjects' choices regarding their personal data.
3. **Respect for context.** We recognise that data subjects' expectations about fair and ethical use of their personal data is informed by the context in which their data was first collected.
4. **Limited sharing.** We limit unnecessary personal data sharing with third parties.
5. **Retention.** We retain personal data only for as long as we need it.
6. **Security.** We ensure appropriate security.
7. **Governments.** We engage with governments responsibly.

Our progress this year

Artificial intelligence and machine learning

Throughout the year we focused on making sure we are using AI and ML in a responsible way for consumers. It is one of the key issues in our business and we work closely with the AI group team to align AI and ML with data privacy and protection. This includes providing training and setting up guidelines for the AI teams and data-privacy leads across the group. The aim is to make sure we are handling data in the right way across the different businesses both in terms of global policy and ethics, and local regulatory requirements and customer expectations. See page 65 for more information.

"Consumer digital businesses are all about providing customers with something that improves their lives, and doing that in a trusted way. Our user growth and retention are predicated on this underlying trust in good, responsible data practices and that includes data privacy."

Justin B Weiss
Global head of data privacy

Building trust

We also focused on making sure users' experiences are positive by honouring their expectations and avoiding unwelcome surprises. Looking after and using data responsibly to deliver on our promises to users builds trust – the key currency of our consumer internet business.

Increasing regulation

The proliferation of regulation around the world beyond the EU's General Data Protection Regulation (GDPR) was another key area for us. Important strategic markets where we operate, such as China, Russia, Central and Eastern Europe, North America, Latin America, India, Southeast Asia, Africa, and the Middle East have advanced the cause of privacy and in many cases have introduced new legislation, which brings additional focus on regulatory compliance.

In the US, letgo focused on making product and procedure changes to comply with the California Consumer Privacy Act (CCPA), which came into force in January 2020.

In Brazil, iFood and other companies inside the Movile group stepped up and formalised their programmes to ensure they are ready to comply with the LGPD, Brazil's General Data Protection Law, which comes into force in the summer of 2020.

Data privacy and protection continued

In India, we expect comprehensive data-protection legislation to come into force soon. We have been working hard to make sure our Indian investments have a strong awareness of the requirements and how they can leverage the group privacy model and expertise.

Raising awareness and understanding
Throughout the year, we significantly increased levels of awareness and understanding around data security and privacy. This included board-level engagement as well as developing and empowering data-privacy leaders across the segment.

Our secondment programme has been a highly effective way to grow our groupwide network of data-privacy leaders, and fortnightly calls are an invaluable opportunity for the network to share knowledge and discuss issues. In addition, we have been raising awareness among all group employees.

Data privacy and security by design
We have also been investing more time and effort in reinforcing our capabilities to address data-privacy and security issues at the design stage of new products and services and changes to operations. Building data privacy and protection in as early as possible is a key part of our commitment as a responsible consumer internet company and we will be increasing our focus on this in the coming year. We are working closely with the AI team on data privacy and security by design and we aim to do more, at scale, in the coming year.

We have been broadening the scale of our capacity as a group and as a collective of individual internet experts to do privacy assessments that anticipate customers' expectations at an early stage of product development.

To do this effectively, we aim to amplify our central data-privacy expertise and best practice with a growing army of data-privacy champions in the businesses themselves. We are empowering people around the world to understand the privacy issues and focus on local consumer-centric expectations and solutions in the most effective ways.

To this end we are keen to pursue a privacy engineering certification programme which will allow people across the different businesses to become qualified in privacy-by-design analysis. We are looking to cultivate this capability in the businesses across the group. It is an initiative in line with our broader groupwide decentralised approach which will help scale and accelerate our privacy by design. We aim to empower the businesses with the skills and resources to forge ahead in building privacy into their products and services at the earliest opportunity.

Camila's story

iFood Data Protection Officer (DPO) Camila Nagano shares her story of championing data privacy and protection in iFood and Brazil.

"Since college, I really liked the subject – I did my thesis on the right to be forgotten. My first contact with real privacy in practice was when Justin came to iFood and he gave a class on privacy 101 and I was amazed, I loved it. Justin proposed a secondment and the legal general counsel, Lucas, appointed me.

So, I went to Hong Kong on secondment in 2017 – it was a total life-changing experience. Besides getting to know the culture of a completely different country in Asia and meeting people from around the group, I learnt everything about privacy – not only how to understand privacy and prepare myself for the International Association of Privacy Professionals (IAPP) exam but also how to present at executive meetings. This was for me a turning point in what I really wanted to do.

I took and passed the IAPP exam in Europe. When I came back to Brazil, the Brazilian General Data Protection Law (LGPD) was due to be implemented the following year and it was interesting to be part of the preparations. Then the law was approved and everything started for real. That's when I stopped doing technology contracts and other roles and I started to be dedicated fulltime for privacy in iFood. I became one of the first Data Protection Officers (DPOs) in Brazil.

Here in Brazil, people don't have the same privacy culture as in Europe. It's very new, so it is much more than a legal role – it's an engagement role, a policy role and a tech role. I spend much more of my time talking with technology people than with lawyers, and that's very interesting for me. The best thing is that I can use all the experience I have learnt from GDPR and the Brazilian law and combine all the best practice.

One thing that also really helps is having biweekly calls with the group DPO network where we can all share experiences and insights.

We got a lot of attention from outside, because we are one of the few 100% Brazilian technology companies developing from scratch the means to be compliant with the privacy laws. We are pioneering a made-in-Brazil data-privacy solution. I'm really proud of it because we are building our privacy protection from zero. We want the best privacy standards for our users, for our drivers and our employees.

The thing I like the most is that it is never-ending work. Because it's not only about making sure we are compliant with LGPD – it's about the culture, policy-making and being the best we can, to keep building users' trust and bring much more value. There are always going to be new products, new technology and new regulation to discuss and to learn and new cases to think about. So, we can always keep improving privacy inside the company and across the country.

I've been invited to a lot of events to speak in the name of iFood. I am also part of a network of privacy professionals in Brazil, trying to plant the privacy seed around the country.

For me the main opportunity in Brazil is to be part of this educational moment, where we can teach people what privacy means, why it's important, how it's a differential in iFood's products and how we are building that to ensure we deliver data privacy and protection. The future is just starting. It's exciting!"