PODCAST

What do UK and EU businesses need to know about data protection in Brazil?

INTERNATIONAL PRIVACY SERIES
produced by LEWIS SILKIN

VANESSA RIBEIRO
Partner at Gusmão e Labrunie

GUSMÃO & LABRUNIE

International privacy series: episode 2 – Brazil

What do UK and EU businesses need to know about data protection in Brazil?

Bryony (00:07)

Hello and welcome to another episode of Lewis Silkin's International Privacy Podcast, the series where we take a practical look at data protection laws around the world and ask, what does your business actually need to know before you launch in a new market?

I'm Bryony Long, co-head of the data privacy team here at Lewis Silkin in London. And today we are looking at Brazil, one of the most exciting and dynamic digital markets in Latin America, and increasingly on the radar for UK and European businesses looking to expand. I'm absolutely delighted to be joined by Vanessa Ribeiro, a partner with Gusmão & Labrunie in São Paulo, who is one of the leading data protection practitioners in Brazil. Vanessa, thank you so much for joining us today.

Vanessa Ribeiro (00:49)

Thank you, Bryony. It's a real pleasure to be here. Brazil is a fascinating jurisdiction for data protection, and I think there's a lot that businesses in the UK and Europe will want to understand. So I'm very happy to walk through it.

Bryony (01:05)

That’s brilliant. So let's start right at the very beginning, Vanessa. For listeners who may know the GDPR inside out, but have never had to think about Brazilian law, can you give us the big picture? What is the main data protection law in Brazil and how does it work?

Vanessa Ribeiro (01:21)

Of course. So Brazil's main data protection law is the LGPD, which stands for Lei Geral de Proteção de Dados Pessoais, or in English, the General Data Protection Law. It was enacted in August 2018 and came into force on the eighteenth of September 2020, with enforcement provisions following in August 2021. So it is a relatively young law compared to the GDPR.

But it's a comprehensive and it's a very much inspired by the European model. The LGPD applies to any processing of personal data carried out in Brazil, or where the purpose is to offer goods or services to individuals located in Brazil, or where the personal data was collected in Brazil. So much like the GDPR, it has a broad extraterritorial ridge. If your business is targeting Brazilian consumers from the UK.

You will almost certainly need to comply. The law is overseen and enforced by the ANDP, Agencia Nacional de Proteção de Dados, which is the Brazil's National Data Protection Authority. Since September 2025, ANDP has been transformed into a fully autonomous federal agency with its own budget and independent decision making powers, which is a significant step in terms of enforcement maturity.

Bryony (02:49)

Okay, well that's really helpful context, Vanessa. And I think our listeners will immediately pick up on the parallels between the GDPR. It sounds like there is a great deal of structural similarity between the new two regimes. But let's dig into it a little bit more. One of the questions that we constantly get asked is, if I'm GDPR compliant, am I most of the way there for Brazil? So let's talk about some of the key similarities and differences, starting with the basics.

How does the LGPD define personal data and sensitive personal data?

Vanessa Ribeiro (03:25)

Sure. The definitions are very close. Personal data under the LGPD is defined as information related to an identified or identifiable natural person, which is essentially the same formulation as Article 4 of the GDPR. Similarly, the LGPD has a concept of sensitive personal data that covers categories such as racial or ethnic origin, religious belief, political opinions, union membership, health and sexual life data, and genetic and biometric data. So, it covers much of the same grounds as the GDPR special categories. There is one notable difference though. The GDPR also specifically restricts the processing of personal data relating to criminal convictions and offences under Article ten. And the LGPD does not have an equivalent provision addressing that type of processing. So that is an area where the GDPR seems to have gone further.

Bryony (04:28)

That is an interesting gap and one certainly to look out for. And so, turning to the general processing principles, obviously under the GDPR we have six well-known principles in Article 5 which lawfulness, fairness and transparency, has purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. Does the LGPD follow a similar structure?

Vanessa Ribeiro (04:55)

It does, but it actually goes a bit further in some respects. The LGPD sets out ten processing principles rather than six. Many of them map very closely onto the GDPR principles. You have purpose limitation, adequacy, necessity, transparency, security, accountability. But the LGPD also includes some additional principles. For example, there is a specific principle of non-discrimination.

Which provides that processing must not be carried out for unlawful or abusive discriminatory purposes. There's also a prevention principle, which is about taking measures to prevent harm from data processing. So, while the spirit is similar, the LGPD arguably has a slightly broader set of foundational principles.

Bryony (05:49)

Okay, I think that non-discrimination principle is quite striking and it's something I think that the GDPR addresses slightly more indirectly. Turning to the legal basis for processing, so we've discussed the principles, so now the legal basis is under the GDPR we have seven legal basis under Article 6 and then we have a special processing conditions where you're processing special category data which are effectively more restrictive. How does that compare with the LGPD.

Vanessa Ribeiro (06:17)

Yeah, good question. So, the LGPD also requires a legal basis for processing personal data, and the framework is similar in concept, but the LGPD actually recognises a broader set of legal bases than the GDPR. The LGPD sets out ten legal bases in its article seven. Many will be familiar. So, we have consent, compliance with the legal obligation, execution of a contract protection of life, legitimate interest, but the LGPD also includes some bases that do not have direct equivalents under the GDPR, such as processing for credit protection, for instance, which is quite specific to the Brazilian market. For sensitive personal data, on the other hand, the LGPD similarly requires a specific legal basis under Article 11. And when relying on consent for sensitive data, it

must be given specifically and prominently. One difference here is that the GDPR requires explicit consent for a special category of data, while our LGPD uses the phrase specifically and prominently. The substance is similar, but the wording differences slightly, and we need to see how the authority and the courts will interpret that requirements.

Bryony (07:40)

Okay, well that is a useful comparison. And consent is often an issue we get asked about. So, I guess let's talk about them, the consent requirements a little bit more generally. GDPR consent has to be freely given, specific, informed and unambiguous. And there's no room for implied or an opt out consent or some people call it form based consent. Is that the same under the LGPD?

Vanessa Ribeiro (08:04)

It is very much so. So, the LGPD requires consent to be freely given, specific, informed, and unambiguous. And the controller is the one who bears the burden of providing that consent was lawfully obtained. There's an additional requirement that if consent is given in writing, it must be presented in a clause that stands out from other contractual clauses. So, Brazil takes the presentation of consent quite seriously.

Importantly, just as under the GDPR , consent is not the only legal basis available, and businesses often rely on other basis such as ledge made interest or contractual necessity where appropriate.

Bryony (08:48)

Yeah, I guess that's actually very similar under the GDPR as well. So, let's talk about a few other areas that we often get asked a lot of questions or certainly companies that we work for like to know about when moving into new markets. First, data protection officers. Under the GDPR, you need a DPO in certain circumstances. So, for example, if you're a public authority or you're an organization carrying out large scale systematic monitoring or large scale processing, special category data, for example.

Does the LGPD have a similar concept and if so, what are the requirements?

Vanessa Ribeiro (09:25)

Yeah, so this is actually an area where the LGPD is broader in one sense, but narrower in another. In principle, the LGPD requires all controllers to appoint a DPO whenever personal data is processed. So, on the face of the statute, it's a wider requirement than the GDPR. However, ANPD has introduced an exemption for small businesses under resolution number two. So, under this resolution, small processing agents that are not engaged in high-risk data processing do not need to appoint a DPO as long as they maintain a communication channel for data protection inquiries. And more recently, ANPD resolution 18 has set out detailed guidelines on DPO responsibilities.

One other difference is that the LGPD does not require processors to designate a DPO, even though it is reputed as a good practice here in Brazil as well. So that's a contrast to the GDPR, where we can see a requirement that processors also appoint in certain situations a DPO.

Bryony (10:35)

Okay, well that is a helpful distinction and good to know it's a little bit more flexible than the regime we seem to have over here. Turning to another hot topic, particularly at the moment in the UK, is data subject rights. So, this is obviously a core area under the GDPR and I guess is fundamental for enabling data subjects to exercise control over how their data is used.

So, we, for example, have rights of access, rectification, erasure, data portability, the right to object, the right to restrict. And very importantly now, we have the right to complain. But how does the LGPD compare?

Vanessa Ribeiro (11:19)

Yeah, so the LGPD provides a similar suite of data subject rights, but there are some differences in detail. So, data subjects in Brazil have the right of access, ratification, erasure, or anonymization. They also have the right to data portability and objection. One key practical difference though is the time scale for responding.

So, under the LGPD, controllers must respond to access requests within 15 days, whereas the GDPR allows 30 days. So, the time frame is tighter in Brazil, which is

something businesses need to be operationally ready for. The LGPD also gives data subjects the right to anonymize block.

Or temporarily suspend any processing that is unnecessary, excessive, or unlawful. This is not quite the same as the GDPR's right to restriction, but it serves a broadly similar protective function. on data portability, both regimes provide for it, but the GDPR sets out more detail on the format and mechanics of portability.

The LGPD leaves much of this to future regulation by the ANPD, which is still pending.

Bryony (12:36)

Okay, well that's — I mean, that's really quite interesting. I mean, 15 days is not a lot at all. We obviously have the 30 days as you mentioned, but then we also have rights to extend as well. So that is definitely something if I was launching in Brazil, I would be making sure I'm operationally aware of. So, the other big area that is particularly topical for us, particularly in light of AI is automated decision making.

And we've got a sort of a recent relaxation, I guess, under the UK law, whereas in Europe, it's very much consent based. you want to do it, unless there's a specific lawful basis you can rely on, whereas in the UK, it's more permissions, but with safeguards. How is automated decision making dealt with in Brazil?

Vanessa Ribeiro (13:22)

Yeah, great. So, both laws address it, but the GDPR provides a stronger standalone rights. Under the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing that produces legal or significant effects with certain exceptions. The LGPD in contrast gives data subjects the right to request a review of automated decisions that affect their interests.

And the right to clear and adequate information about the criteria and procedures used. However, this provision does not establish that this review will be conducted with human intervention. It was actually in the law when it first came out, but then there was a revision of the law not to specifically require human intervention.

The ANPD has been increasingly active in this area. The ANPD's president has publicly stated, for instance, that Article twenty of the LGPD, the one handling automated decisions, already gives the authority a basis to address automated decision making in the context of AI, even ahead of any dedicated AI legislation here in Brazil.

Bryony (14:37)

Okay, that's really practical insight for businesses deploying AI powered tools in Brazil and one that I think will require some further thinking to successfully implement.

So, Vanessa, one thing that you've mentioned a couple of times is having certain clauses and contracts. In the GDPR under Article 28, there are specific provisions that all data processing agreements must contain. Is there a similar type of requirement under Brazilian law?

Vanessa Ribeiro (15:04)

Yeah, we don't have that level of specificity in the Brazilian law currently, but we do have some guidelines from the Brazilian authority suggesting or recommending better said that companies would implement data processing agreements with their data processors and suggesting a couple of things that companies should pay attention to. So, in this arena I would definitely have a Brazilian attorney reviewing the contract if your processor is in Brazil or if you're doing something that falls within the scope of the Brazilian law just to make sure that your contract also complies with everything it's needed here in Brazil.

Bryony (15:48)

Okay, perfect. So, moving on to data security, one again, another very hot topic for us and breach notification. How does the LGPD compare with the GDPR here?

Vanessa Ribeiro (16:02)

So, on data security, both laws require appropriate technical and organizational measures to protect personal data. The GDPR goes into somewhat more detail, including specific provisions on data protection by design and by default. The LGPD does not use the freight, for instance, data protection by design and by default expressly, but it does include very similar requirements.

In the sense that controllers must implement appropriate measures from the conception of a product or service through to its execution. So, on breach notification, this is an area where businesses need to pay careful attention. Under the GDPR, controllers must notify the supervisory authority within 72 hours of becoming aware of a breach, there's likely to pose a risk to individuals.

And must notify affected individuals without undue delay if there's a high risk. Under the LGPD, as clarified in resolution 15 of the authority, controllers must notify both ANPD and affected data subjects within three business estates from the date of the controller. so let me do we do that.

So the controllers must notify both the authority and affected data subjects within three business days from the date of the controllers from the day the controllers learn about the breach that may pose risk or relevant harm. So ~ it seems a Brazilian clock to start from knowledge of the breach and the window to notify is three business days rather than seventy-two hours, which might not be the same depending on the on the day of the week you gain knowledge, right?

Bryony (17:48)

Well, that sounds pretty similar to what we have over here. So, moving on, another interesting topic, data transfers. Now, this is one area that I particularly want to explore because it's been one of the most significant developments in recent months, and that's international data transfers.

How does Brazil handle cross-border transfers? I guess the big news, what is the current status of EU adequacy for Brazil?

Vanessa Ribeiro (18:14)

Yeah, so this is where we have had some great progress indeed. So let me start with the framework. Under the LGPD, cross-border transfers of personal data is allowed under specific circumstances. The permitted mechanisms are very similar to the ones under the GDPR. So, transfers are allowed where the recipient country has been recognized as providing an adequate level of protection.

Or where appropriate safeguards are in place, such as the standard contractual clauses or biding corporate rules. In August 2024, ANPD published Resolution 19, which established detailed rules on ~ international data transfers, including the ~ ANDP's own approved SECs, the standard contractual clauses. On 27 January 2026, the European Commission and Brazil adapted mutual adequacy decisions. This means the EU has formally recognized that Brazil provides a level of data protection essentially equivalent to that of EU, and Brazil has reciprocally recognized the EU through ANDP resolution 32 of 2026, so quite recently. The practical effect is that personal data can now flow freely between the EU and Brazil without the need for additional transfer safeguards.

Such as Santa Contractual Clauses.

Bryony (19:37)

Yeah, now I saw that the European Commission described it as creating the largest area of free data flows in the world covering over 670 million people across the EU and Brazil. So, it's a pretty significant agreement. And I have to say though, for those UK listeners, unfortunately this is an agreement between the EU and Brazil. So, at the moment that doesn't extend to the UK.

Which means that if you are transferring data outside of the UK to Brazil, you would still need to think about putting in place standard contractual clauses or considering another mechanism. I did have one question for you, Vanessa. So, you did obviously mention the fact that you have the kind of Brazilian SECs. For some of our clients who ~ try and adopt a more globally agnostic approach to international transfers, particularly in their intergroup data transfer agreements. Some of them may continue to rely on European SCCs from to transfer data out of jurisdictions where they may not have similar STCs in place. Is it at all market possible for organizations to rely on EU SCCs to transfer data out of Brazil back to the UK just to avoid having to add Brazilian SCCs, for example, into their data sharing or their intergroup data sharing agreements.

Vanessa Ribeiro (21:04)

Yeah, so the current position is that so like the straightforward answer would be like no. It won't be like the best practice, especially because in the Brazilian SECs there are like a couple of clauses that the authority request that are not changed into the agreement at all. And some others that you still have some flexibility. So, for such certain clients at

least who want to take advantage of the European SECs, what we are trying to do is that to make sure that at least those blocks of clauses that the Brazilian authorities require, they are reflected into those agreements. So, in a way we're trying to interfere the least possible that we can do, right? But also make sure that we don't get in trouble with the authority by failing to put on any of the clauses that the authority told us, right? Or recommended there are in place.

Bryony (22:01)

Yeah, I understand that. Do you ever find that you can incorporate them by reference? So again, over here, when we're incorporating SECs into our contracts, rather than have the full 14 pages of the SECs appended, sometimes we incorporate them by reference. So, we simply cross refer out to them. Could you do a similar thing with the Brazilian SECs?

Vanessa Ribeiro (22:24)

Yeah, there's no restriction on that. So, I think there's still room for you to approach the matter in this sense. And still. Yeah.

Bryony (22:33)

Okay, perfect. Well, that's good to know.

Okay, brilliant. So last time we saw each other, we did have a little chat about children's data. And I just wanted to sort of move on to that because it's obviously a very big topic again for us over here. And I think a very big topic in Brazil too. In the UK, we obviously have our age-appropriate design code. And we've now recently got our online safety act, which has introduced new duties for platforms. What's been happening in Brazil around this space?

Vanessa Ribeiro (23:02)

Yeah, so that's definitely a hot topic. So, Brazil has been extremely active in this space, arguably even more so than many other jurisdictions, including Europe or the UK, perhaps. Starting with the LGPD itself, Article fourteen provides that personal data of children must be processed in their best interest, which is a constitutional provision as well. For children under the age of twelve. The LGPD requires the specific and

prominent consent of at least one parent or legal guardian. However, LGPD has clarified through its statement one of May 2023 that controllers may also rely on other legal basis for processing children's and adolescents' data under Article 7 and 11 of the LGPD, provided the best interest of the minor takes precedent, which is, as I said, a constitutional command.

Bryony (24:00)

Okay. So, again, I guess pretty similar to us in that there are various legal basis, but if you are relying on consent, specifically in connection with information society service, then you need to get parental consent if the child is under the age of 13. similar 12 and 13 approaches are taken. So I think what the other piece of news that I saw was about the new digital ECA. you care to talk a little bit about that and what that's bringing to Brazilian law?

Vanessa Ribeiro (24:34)

Yes. So, I don't always subject to the overriding requirement that the child's best interest must prevail. The real big development here in Brazil is the digital statute of the child and adolescent act, which is the digital ECA, or as we say here in Brazil, ECA. It was enacted on the 17th of September 2025 and came into force recently on the 17th of March 2028.

So, the digital ECA is one of the most I would say comprehensive online child protection laws in the world. It applies to all information technology products and services there are directly at or likely to be accessed by children under twelve and adolescents between then twelve and eighteen. So, the concept of likely to be accessed is deliberately broad in the law. It looks at the probability of use, ease of access, attractiveness to minors and potential risks. So, you cannot simply say for instance our service is not designed for children. If in reality children are likely to use it, then you are subject to the law and you need to comply with a bunch of things.

Bryony (25:43)

Okay. Well, I mean, I guess that is quite similar. We have the concept of likely to be accessed under the age-appropriate design code. And that certainly is quite similar how you've described the approach that the ICO would certainly take. It's just the differences that ours is a code of practice, code of best practice as opposed to law.

You mentioned that there are a bunch of different requirements that you would need to comply with if you're caught under ECA. Could you give a few examples of what those might be?

Vanessa Ribeiro (26:14)

Yeah, sure. So, providers must implement safeguards at the design stage and throughout the product's life cycle, ensuring the highest level of privacy and data protection by default. They must also clearly inform users about age classification policies. They must adopt appropriate technical measures, including industry recognized scrutiny measures to enable families and guardians to prevent inappropriate access. The digital ECA specifically prohibits the use of profiling techniques for targeting commercial advertising to minors. That's a very interesting obligation. It also prohibits the use of let's say emotional analysis, augmented reality, extended reality and virtual reality for advertising purposes involving children and adolescents. Another thing for instance, and it's big for the game industry, so loot boxes those randomized reward mechanisms in games, they are banned under the digital ECA for services directed or likely accessed by minors.

Bryony (27:19)

Okay, so they have very specific and I would say quite far-reaching prohibitions. So, what about enforcement?

Vanessa Ribeiro (27:27)

Yeah, so the penalty is indeed significant. So, fines can reach up to ten percent of the offender's economic group revenue in Brazil from the prior fiscal year, or if the revenue data is not available, a fine ranging from ten to one thousand reais per registered use, capped at fifty million reais, which is approximately nine to ten million US dollars per violation per use depending on the circumstance. The ANPD has been designated as a primary enforcement body and has already signalled that monitoring compliance with the digital ECA is a top priority for 2026 and 2027. In 2026 according to the agenda published by the authority, the focus will be on inspecting how processors comply with the requirements, including age verification mechanisms. By 2027 they expect to expand enforcement took over privacy by design and parental supervision tools.

Bryony (28:32)

Okay, wow. So, it really is very much a live enforcement priority and it's certainly not a law that's just sitting in the statute books. So, I think it's safe to say that it's really important for any businesses with a digital product or service that could be accessed by young people in Brazil to really pay attention to this law. And I guess it doesn't come to any surprise to our listeners over here. We're seeing a lot more increased action, particularly from the ICO with then fining Reddit and then there was Media Lab and then we've got Ofcom who are fining many adult websites who've not been prevented access by children. But it certainly is, along with the EU as well, a regime that's coming down very hard on non-compliance when it comes to children's data. Certainly, I would be very mindful if I was launching a child accessible product in Brazil to make sure I was fully aware of those provisions.

Iguess now before we wrap up, what I'd love to do is just spend a few minutes just looking at kind of red flags and guess kind of practical watch outs. So those things that might catch someone in the UK or the European business off guard when they start operating in Brazil. If you were advising a business launching in Brazil, what would your top areas of concern be for them?

Vanessa Ribeiro (29:52)

Yeah, so great question. I would definitely highlight several areas.

First, the shorter response times. As we discussed, you only have fifteen days to respond to data subject access requests under the LGPD compared to the thirty days under the GDPR. And for breach notification the window is a bit longer, let's say three business days from knowledge of the incident. So, if your incident response process is calibrated for GDPR timescale,

Or the data subjects' response times you probably need to pay attention to the Brazilian requirements. Second, the DPO requirement is broader in scope under the LGPD. In principle, all controllers must appoint a DPO unless the small business exemption applies. So even if you don't need a DPO under the GDPR

You may still need one for your Brazilian operations. Third, be aware that while the LGPD does not explicitly require written data processing agreements in the way that Article 28

of the GDPR does, ANPD has issued guidance strongly recommending them. So best practice is to have written agreements with your data processors in Brazil, even if the law doesn't mandate some level of contractual detail.

Fourth thing that I would like to highlight, legitimate interest as a legal basis works somehow differently in practice. The ANPD requires that where a controller relies on legitimate interest, a balancing test is carried out and in certain risk situations also a data protection impact assessment is carried out.
So fifth, and this is increasingly important, be very careful about AI and automated processing in Brazil. ANPD has been proactive in enforcing the LGPD against major technology companies, including preventive measures against Meta, actions against TikTok on age verification for minors, and regulation of biometric data collection by Sam Altmann's Tool for Humanity Project.

The ANPD has shown it will act swiftly and it's not intimidated by the scale of international technology companies. That said, and just as a general compliance principle, we recommend avoiding also jurisdiction specific privacy practices whenever possible, and instead adopting a harmonized global approach based on the highest applicable standard. This approach not only reduces compliance complexity and operational burden.

But also aligns with what seems to be the expectation of the ANPD, which has consistently emphasized transparency, meaningful user choice, and effective exercise of data subject rights. Notably, in its review of WhatsApp 2021 privacy policy update, the ANPD scrutinized whether users in Brazil were provided with the time, with the same level of transparency and user facing controls as in Europe, for example, and took an issue with the fact that the Brazilian data subjects were not. So that's where this recommendation whenever possible comes from.

Bryony (33:17)

Okay, well that is a really important point. And I think I would add just from listening in is that the UK from a UK EU GDPR perspective that I think businesses should not automatically assume that their existing GDPR compliance programme will also automatically cover them in Brazil. I think while there's clearly a high degree of alignment between the two frameworks, there are differences in the detail.

Just noting down from this podcast, there are additional processing principles, there are broader DPO requirements, the tighter response times for DSARS in particular, and then

obviously there's very specific children's status rules under ECA. And then obviously the ANPD's increasingly assertive enforcement posture on that mean that you really do need to conduct a proper gap analysis and make sure that your Brazilian compliance is fit for purpose before launching.

Vanessa Ribeiro (34:11)

Yeah, I completely agree, Bryony. And I would add one more practical watch out. With a mutual adequacy decision now in place between the EU and Brazil, businesses may be tempted to simplify their transfer arrangements. And rightly so, right? But they should not overlook the fact that adequacy decision will be reviewed. They should also check carefully whether any particular transfer generally falls within the scope of the decision.

And whether any onboard transfer issues arise. It may also be sensible to have a fallback mechanism in there with the Brazilian SECs, for instance, in case there is a successful challenge to adequacy in the future. And as you mentioned, Bryony UK businesses are not covered by the EU Brazilian adequacy decision and will need to maintain their own transfer mechanisms. as I said before, the mechanisms provided for under the Brazilian law are very similar to the ones under the GDPR, they can rely on BCRs, SECs or other transfer mechanisms that are available under the LGPD.

Bryony (35:15)

Yeah, perfect. And similarly, we have a similar sort of concept of, you know, where we've agreed adequacy or, or where, you know, there's sort of extensions to European adequacy decisions. We also often have those fallback positions, because as we all know, these adequacy decisions are a little frail at times, to say the least.

So, I think in conclusion, coming to the end of this, Brazil is certainly a market with a very sophisticated and increasingly mature data protection framework and that obviously shares a great deal of DNA with the GDPR but obviously has its own distinctive features and from what sounds like an increasingly active regulator. So, I think any business considering launching in Brazil should invest in understanding the LGPD and the digital ECA properly to ensure that for operational purposes that they're aligned with those tighter Brazilian time scales and they obviously take the regulators enforcement appetite very seriously.

Vanessa Ribeiro (36:13)

Yeah, Brazil is definitely a lot of fun, let's say. So, thank you, Bryony. We are always happy to assist business navigating the LGPD, digital ECA and the wider Brazilian regulatory landscape. Any questions, please do feel free to reach out. It's been a real pleasure joining you today.

Bryony (36:32)

Well thank you too very much Vanessa, it's been a real treat to listen to you and hopefully our listeners will agree. I think you've really clearly explained all the differences and hopefully a lot of people will feel a lot more confident about understanding the ins and outs of Brazilian data protection law. As I say, hope turning to our listeners, I hope you found this episode useful. We will be doing other jurisdictions as well. I think we have India for example coming up in our next one.

So do subscribe wherever you get your podcast and we'll see you next time for the next instalment of our International Privacy Series. So, until then, goodbye.

Vanessa Ribeiro (37:09)

Goodbye everyone.