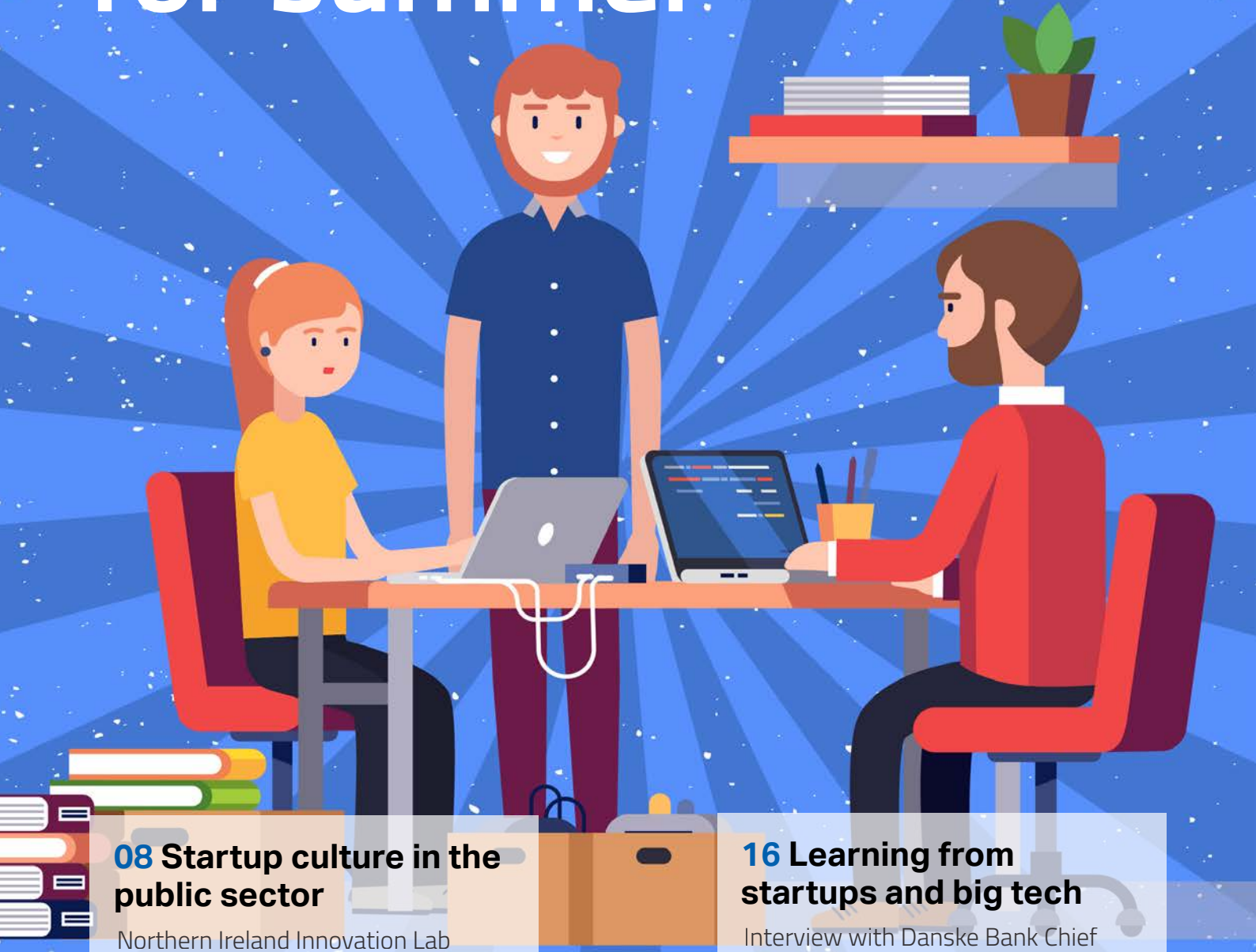
sync ni magazine

www.syncni.com

Tech for good 06
Blockchain 10
AirPOS 22
GDPR for startups 28

Startups in focus for summer



08 Startup culture in the public sector
Northern Ireland Innovation Lab

16 Learning from startups and big tech
Interview with Danske Bank Chief Digital Officer Søren Rode Andreasen

legally obliged to comply. The right to be forgotten is not absolute; your right to retain the data may override the rights of the data subject.

If you hold any data for marketing purposes then remove the individual from your mailing list. If your lawful basis for processing relies on consent, start deleting!

The GDPR doesn't specify what 'erasure' means, whether it means destruction of the data or anonymisation. If you have to comply with a request, the Information Commissioner's Office's guidance on deleting personal data indicates that they will take a pragmatic approach and that the obligation will be met so long as the information by which the individual can be identified is put 'beyond use'.

My app has customers all around the world, meaning I use servers positioned all over the globe. What does the GDPR say about this?

The GDPR prohibits the transfer of personal data to 'third countries' – this means countries outside the EEA (which includes the EU, Iceland, Liechtenstein and Norway) – except in certain circumstances: (i) if the transfer is to a territory which the EU has listed as having adequate data safeguards; (ii) if approved safeguards have been put in place between the transferring and receiving party; or (iii) if the transfer falls within one of the derogations allowed in specific circumstances.

Here are three possible approaches (which aren't mutually exclusive). No matter how you decide to approach the transfer, it's worth remembering:

- if you're acting as a processor you will always need the consent of the controller and this can be managed in your terms of business;
- you'll need to make the fact of the transfer clear in your privacy notice and explain why it's permitted;
- don't forget that the hosting services provider is another link in the chain: it's a sub-processor and you'll need to make sure it's contact with you conforms with the GDPR.

Option 1: *Only use servers in places which have been deemed safe or have self-certified.* Restrict your transfers to servers based in the EEA or countries for which the EU Commission has made an adequate data safeguards decision (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay) or transfer to servers in the US provided by companies registered under the EU-US Privacy Shield.

Option 2: *Implement appropriate safeguards through your contracts.* If you need to use servers in territories outside those listed under option 1, or to a US company which hasn't signed up to Privacy Shield, you could consider adding 'model contract clauses' (downloadable from ec.europa.eu) to your terms of business. However, they may be of limited benefit to most app businesses since the available clauses don't yet include the processor-to-processor provisions you'd need to manage data on behalf of your customer as a processor.

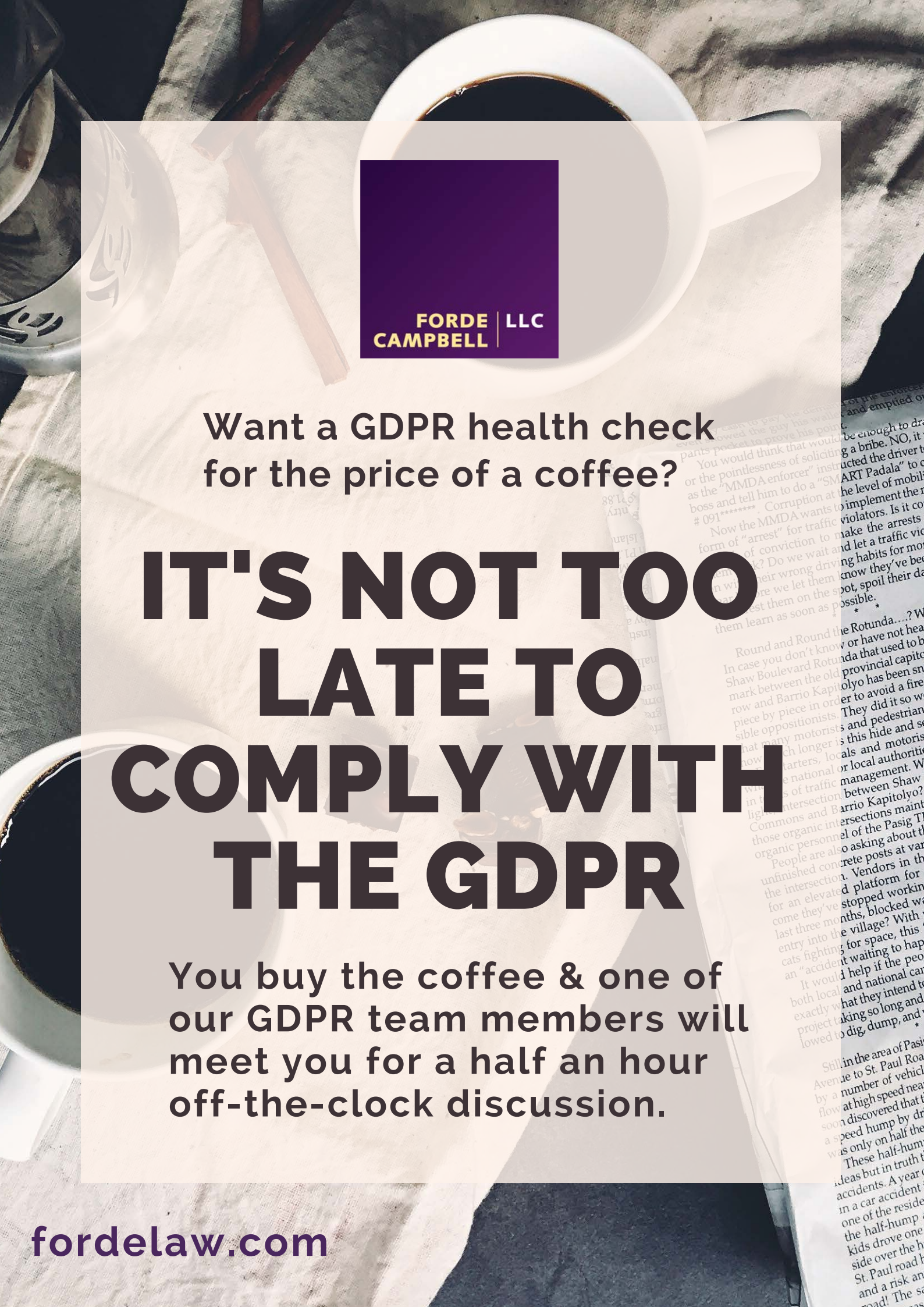
You could also set up a subsidiary company in the country in which the servers will be based and enter into a data processing agreement with that subsidiary, undertaking a permitted transfer in reliance on 'binding corporate terms'. These terms are freely available online, but since the GDPR imposes restrictions on onward transfer to third countries, this option is limited.

Option 3: *Derogations for specific situations.* If neither option 1 nor 2 work for all of the territories in which you need servers, then you should consider whether any of the eight derogations set out in Article 49 of the GDPR apply.

For the purposes of your app business, Paul, it is likely that the only viable option would be to obtain the explicit consent of the data subject to the transfer of their data, having explained the risks.

In a B2C model the user can freely decide if they want to use your service or not. But in a B2B model where the app is licensed by a company with its employees as designated users, given the asymmetric structure between an employer and its employees, the courts may be reluctant to deem any such consent as freely given.

Forde Campbell LLC have shared this conversation in a bid to fill in gaps between principle and practice. GDPR is a new law in a very big space. It is as yet untested and each business will need to find its own path. Don't rely on this article as a definitive guide or as legal advice. Read it, have a think and drop a note to katey@fordelaw.com and hello@paulmcbride.net if you have further questions or want to be part of the continuing conversation.



FORDE CAMPBELL | LLC

Want a GDPR health check for the price of a coffee?

IT'S NOT TOO LATE TO COMPLY WITH THE GDPR

You buy the coffee & one of our GDPR team members will meet you for a half an hour off-the-clock discussion.

fordelaw.com