MASON HAYES & CURRAN

Digital Health Annual Review 2020

ISSUE 1 – JANUARY 2021

MHC.ie

Introduction

Welcome to Mason Hayes & Curran LLP's Digital Health Annual Review 2020

The global Digital Health market size is expected to reach €683.75 billion by 2027. However, the old Peter Parker adage rings true – with great power comes great responsibility. In the six months since publication of our 2020 Mid-Year Review, advancement in the technology and legal regulation of digital health products has continued apace.

The term Digital Health covers everything from consumer wearables to electronic health records, telemedicine and genomics. The U.S. Food and Drug Administration (FDA) describes the advancement of Digital Health technologies as "leading to the convergence of people, information, technology and connectivity to improve health care and health outcomes". The FDA itself has highlighted the importance of the sector by launching a Digital Health Center of Excellence in September 2020.

Meanwhile in the EU, throughout 2020 we have seen increased focus on the impact of Brexit, the regulation of artificial intelligence (AI), the Medical Device Regulation (MDR) and data privacy issues.

In Brexit news, the transitional period where EU law continued to apply to the UK as an EU Member State ended at 11pm (GMT) on 31 December 2020. We discuss some of the key regulatory changes which will form part of the post-Brexit commercial landscape.

In October last year, the European Parliament voted on a new legislative proposal for a civil liability regime for AI and we examine the potential impact of this for AI "operators". It also proposed a regulation that will seek to manage and control those novel aspects of AI that make it AI, such as autonomy and adaptability. That proposal sets out to tackle big themes and issues like how to ensure safety, transparency and accountability, prevent bias and discrimination, foster social and environmental responsibility, and ensure respect for fundamental rights. High-risk AI applications in the Digital Health sector are a key target of this proposal.

The upcoming implementation of the MDR in May 2021 is quickly approaching. In the meantime, the European Medical Devices Co-ordination Group (MDCG) has published 29 guidance documents this year of particular relevance to Digital Health companies.

In terms of data protection and privacy, various significant measures have been introduced throughout the EU as part of the battle against COVID-19 that have resulted in a significant increase in the collection of data relating to individuals' health, location and social habits. With this, data protection and privacy remains a key issue for Digital Health technology.

In this review we aim to discuss these key issues arising with Digital Health and we hope you enjoy the first edition of our Annual Digital Health Review.

Editors

Michaela Herron
Partner, Product Regulatory & Liability
mherron@mhc.ie

Michaela is a Regulatory Partner who leads the Products practice. She advises clients in the pharmaceutical, healthcare, medical device, digital health, cosmetic, video game, software and general consumer product sectors on various regulatory compliance matters. She has particular expertise in wearables and software medical devices. She frequently advises clients on the applicable regulatory framework, regulatory approval, labelling, packaging traceability, safety and liability issues.

Michaela also represents manufacturers in product liability claims and enforcement action by regulators.

Brian McElligott
Partner, Intellectual Property & AI
bmcelligott@mhc.ie

Brian is a Partner in our Intellectual Property Law team and leads the AI practice. He resolves complex IP and technology issues for clients from a range of sectors including food, beverage, energy, agriculture, pharma, med-tech and eHealth. He works closely with clients on the formulation and implementation of effective IP development and protection strategies.

Brian guides international brand owners through complex IP protection and commercialisation issues and advises major technology companies on IP licensing and due diligence surrounding mergers, acquisitions, IPOs and inward investments.

Contents

The Medical Devices Regulation: Where are we now?

Michaela Herron
Partner,
Product Regulatory & Liability
mherron@mhc.ie

Introduction

The Medical Devices Regulation (MDR) represents a significant development of the existing regulatory system for medical devices in Europe and will replace existing Directives which have been operative for over 25 years. As a Regulation, rather than a Directive, this EU legislation will be directly applicable without requiring transitional national legislation. This should provide for greater legal certainty and prevent variation in the approaches adopted between Member States.

The new Regulation seeks to overhaul the EU regulatory framework for medical devices, with the aims of improving clinical safety and creating fair market access for all manufacturers. Originally, it was set to come into force on 26 May 2020, however, largely due to COVID-19 this date has been extended by 12 months. This means that the MDR will now be fully applicable from 26 May 2021. The implementation of the In Vitro Diagnostics Medical Devices Regulation (IVDR) will also follow a year later and will be enforceable from May 2022. As a follow on to our previous articles tracking this important development, we examine what the MDR seeks to achieve and the position we have gotten to so far in advance of the revised date of implementation.

The MDR's goal

The MDR addresses concerns over the assessment of product safety and performance by placing stricter requirements on clinical evaluation and post-market clinical follow-up, and by imposing enhanced requirements regarding traceability of devices throughout the supply chain. Manufacturers will be required to demonstrate that their medical device meets the relevant requirements through conducting conformity assessments which are dependent on the classification of their device. Once a product has passed the conformity assessment, only then can a CE marking be affixed. Notified Body approvals under these conformity assessments are required for Class IIa, IIb and III devices. Some Class I devices will require a conformity assessment by a notified body for parts relating to sterility or metrology.

The new MDR now requires total life cycle traceability between all stages of product development and post-market activities. Companies with low-risk Class I devices are required to produce a post-market surveillance report.

Labelling requirements have also been overhauled. General Safety and Performance Requirements (GSPR) checklists have been mandated. Information on warning, precautions or contraindications on devices have also been made mandatory as part of the labelling process. Labels require the EC representative's name, address and symbol. Additionally, clinical evidence is now required for all medical devices. This involves extensive clinical testing in some cases.

The Corrigenda

There have been two corrections or corrigenda to the MDR.

The first Corrigendum was published in May 2019 in the Official Journal of the European Union (OJEU) and related to amending linguistic and other minor errors.

The second Corrigendum was prepared by the Council of the EU on 3 December 2019. This correction of the MDR amends Article 120, entitled the "Transitional provisions". It permits manufacturers of Class I devices under the Medical Devices Directive (MDD), who will be up-classed under the MDR, to avail of a four-year transitional period. Accordingly, manufacturers will be able to place these devices on the market until May 2024 and are further allowed to make these devices available to end-users until May 2025. In order to avail of these transitional provisions, a device must obtain a CE marking as a Class I device under the MDD before 26 May 2021. In addition, no significant changes can be made to the intended purpose and design of relevant devices past 26 May 2021. Further guidance has been published on Article 120 by the Medical Device Coordination Group (MDCG), as discussed in further detail in a separate article in the Review.

Notified Bodies

The MDR has significantly increased the requirements which must be fulfilled before being designated as a notified body.

These new requirements relate to organisation and general requirements, quality management requirements, resource requirements and process requirements. The designation process involves national and European assessments, which can take up to 18 months to complete.

At the end of January 2020, over 85% of European Notified Bodies currently operating had applied for designation under the MDR, however at present, there are only 17 accredited notified bodies across Europe.

With 47 Notified Bodies still in the process of obtaining designation under the MDR, concerns had arisen about these organisations' capacity to support medical device manufacturers' European certification requirements past the original May 2020 compliance deadline. The one-year delay was hoped to have provided much needed time for pending submissions to get accreditation, however, there are still a significant number of Notified Bodies who are yet to receive MDR designation.

MDCG guidance documents

Throughout 2020 the MDCG has continued to publish guidance documents to assist stakeholders in implementing the MDR and with the objective of ensuring uniform application of the relevant provisions of the MDR. Since our last update, the MDCG has issued further guidance, bringing the total to over 60 documents, including the following published in the last few months:

- A Position paper on the use of the EUDAMED actor registration module and of the Single Registration Number (SRN) in the Member States
- Guidance for notified bodies on the use of MDSAP audit reports in the context of surveillance audits carried out under the MDR/IVDR, and
- Questions and Answers on MDCG 2020-4: Guidance on temporary extraordinary measures on medical device notified body audits during COVID-19 quarantine orders and travel restrictions

EUDAMED

EUDAMED is a database designed to centralise and organise information on medical devices placed on the European market and is a critical component of the regime provided for under the MDR and IVDR. The European Commission launched the first of six planned modules making up the EUDAMED database in December 2020.

This first Actor Registration Module is addressed to the registration of economic operators and requires that manufacturers, authorised representatives and importers of MDR compliant devices (Actors) register their organisations and devices with their Competent Authorities. The Actor Registration Module is a prerequisite for the use of the other EUDAMED modules and facilitates a secure way of accessing EUDAMED. In August 2020 the MDCG published a position paper on use of the Actor Registration Module and a "frequently asked questions" document explaining the registration process was also released by the European Commission in December 2020.

Conclusion

The MDR seeks to significantly change the regulatory environment for medical devices with traceability, safety and proven usability at the forefront. The new Regulation is far more rigid and so, with only a few months to go, industry players should continue to prepare themselves for the 26 May 2021 deadline.

Legislative Update: Product Liability & Safety in Focus

Michaela Herron
Partner,
Product Regulatory & Liability
mherron@mhc.ie

Rebecca Dowling
Associate,
Product Regulatory & Liability
rdowling@mhc.ie

Product Liability Directive

The Productive Liability Directive 85/374/EEC (PLD) was originally adopted in 1985 and established a European wide system of strict liability for people to claim compensation for damage caused by defective products. However, given the accelerating development of technologies such as AI and machine learning, existing EU and national legal frameworks on product liability, of which the PLD forms an important part, may no longer be fit for purpose. One of the constant questions over the last number of years is whether the PLD can or should cover standalone software products. For example, a November 2019 report of the European Commission's Expert Working Group on New Technologies entitled "Liability for Artificial Intelligence and other emerging digital technologies" raised concerns on whether the existing definitions of damage and defect were sufficiently encompassing given the new technologies existing in consumer products on the market.

Most recently in October 2020, a report setting out MEP recommendations to the European Commission on how AI should be regulated in the area of civil liability was adopted by the European Parliament. This report set out a number of proposed changes that would potentially impact on the PLD:

- Calls for the European Commission to consider transforming the PLD into a regulation, and to review the definition of "product" as well as concepts such as "damage", "defect" and "producer"
- A new regime for civil liability claims of individuals and corporations against so-called "Operators" of AI systems
- A system of joint and several liability in cases involving more than one Operator, with rights of recourse amongst Operators in such a scenario to apportion liability as appropriate
- Further consideration of the concept of "time when the product was put into circulation" given that some AI systems can iterate and evolve through the use of self-learning algorithms over the course of their lifecycle

- The creation of a strict liability regime for Operators of "high-risk" AI systems, with a definition of "high risk" as *"significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used".* All high-risk AI systems would be listed in an Annex to the proposed regulation, which would be revised regularly

Feedback from the European Commission is awaited. In time however, providers of AI systems may be required to consider if they satisfy a definition of Operator, and perhaps more importantly given the possible application of strict-liability, if their AI system(s) can be classified as "high risk".

The European Commission is set to tackle a review of the PLD in the first quarter of 2021.

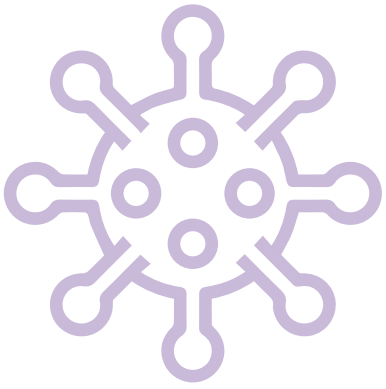
General Product Safety Directive

The General Product Safety Directive 2001/95/EC (GPSD), adopted in 2001, is the central piece of EU legislation providing a "safety net" of requirements for general consumer products across all EU Member States. The various requirements and obligations set out in the GPSD are designed to ensure that all products placed on the EU market are safe, and that consumers are sufficiently informed about the products that they purchase and use, even if those products are not within the scope of sector-specific EU legislation. As the nature of the products that we use and the way that we use them changes over time however, so too must product safety legislation.

In recognition of this requirement, the European Commission's 2020 working programme has stated as part of its regulatory, fitness and performance programme (REFIT) that it will carry out a review of the GPSD in the second quarter of 2021. Similar to the PLD, there has been commentary on whether the GPSD should instead be replaced by a Regulation. There have been similar concerns raised about the lack of clarity surrounding the GPSD and whether it can or should apply to software products. It is hoped that this issue will be clarified during this year's review.

The Commission's public consultation stage closed in early October. While a further update is awaited, the European Parliament's Committee on the Internal Market and Consumer Protection adopted an own-initiative report in October 2020 calling for aligned market surveillance rules for both harmonised and non-harmonised products placed on the market offline or online. In November 2020, the Commission also launched the New Consumer Agenda, which along with green and digital policy, also focuses on the modernisation and harmonisation of existing consumer protections, particularly for the online retail space.

Changes to both the GPSD and PLD will need to be monitored very carefully by Digital Health companies given that they are the pillars of the product safety and liability regime in the EU.



At a Glance: Upcoming EU Law Developments

James Gallagher
Senior Associate,
Product Regulatory & Liability
jamesgallagher@mhc.ie

The following legislative milestones and wider policy proposals will be a feature for digital health companies in 2021:

The full application of the MDR on 26 May 2021

The publication of the Sale of Goods Directive (EU) 2019/771 and the Digital Content Directive (EU) 2019/770, which must be implemented by Member States by 1 July 2021, with national implementing measures to take effect from 1 January 2022

The publication of the Enforcement and Modernisation Directive (EU) 2019/2161 (aka the Omnibus Directive) which must be implemented by Member States by 28 November 2021, with national implementing measures to take effect from 28 May 2022

An upcoming review of the Product Liability Directive 85/374/EEC by the EU Commission in Q1 2021

The publication of the Regulation on Market Surveillance and Compliance of Products (EU) 2019/1020, applicable from 16 July 2021 for the most part, with Articles related to the establishing of the Union Product Compliance Network already in effect from 1 January 2021

The publication of the Accessibility Requirements for Products and Services Directive (EU) 2019/882, which must be implemented by Member States by 28 June 2025

An upcoming review of the General Product Safety Directive 2001/95/EC by the EU Commission in Q2 2021

Support for a "Common European Health Data Space" as set out in the European Strategy for Data, adopted in February 2020, and the publication of a proposal for a Regulation on European Data Governance, published on 25 November 2020

Proposals to introduce specific further conformity assessment requirements and legislative regimes for certain "high-risk" AI applications, contained in the Commission's White Paper on AI, as well as the publication of the Report on safety and liability implications of AI, IoT and Robotics

The full application of Regulation 2017/746 on In-Vitro Diagnostic Devices (IVDR) on 26 May 2022

EU Directive on Representative Actions: A Future Concern for Digital Health Providers

John Farrell
Partner, Commercial & Technology
jfarrell@mhc.ie

Michaela Herron
Partner, Product Regulatory & Liability
mherron@mhc.ie

Emma Maher
Associate, Commercial & Technology
emaher@mhc.ie

EU Directive 2020/1828 on representative actions for the protection of the collective interests of consumers (Directive on representative actions) was published in the Official Journal on 4 December 2020. Once it comes into effect, it will harmonise the regime for collective actions to be brought on behalf of EU consumers. It also aims to balance the availability of the mechanism across Member States while providing safeguards to prevent frivolous claims against traders.

Qualified entities

The Directive on representative actions will require each Member State to designate at least one "qualified entity" to bring actions on behalf of consumers. A list of qualified entities will be maintained by the European Commission. Qualified entities such as consumer organisations will be empowered to bring collective action cases on behalf of consumers for breaches of a wide range of EU directives and regulations. Member States will have a high level of discretion in selecting the criteria that qualified entities must meet for the purpose of bringing domestic representative actions.

In order to bring a cross-border representative action, the qualified entity will have to meet certain criteria:

- Be a non-profit organisation in the area of consumer protection
- Be independent, and
- Have a legitimate interest in ensuring the provisions of the Directive are complied with

The Competition and Consumer Protection Commission is likely to be a qualified entity in Ireland.

The Irish position

At present, there is no mechanism under Irish law for collective redress or class actions to be brought on behalf of consumers. Once implemented, the Directive on representative actions will require Ireland to introduce at least one representative action procedure for injunction and redress actions which can be brought by qualified entities.

Impact on the digital health sector

The infringement by traders must be related to a limited set of European directives and regulations specified in Annex I to the Directive, along with their national implementing measures. Of particular interest for the digital health sector is that the following areas are covered:

- The General Product Safety Directive
- The Digital Content Directive
- The Sale of Goods Directive
- The GDPR
- The Directive on liability for defective products
- Medical Devices Regulations, and
- EU Regulations on medicinal products for human use

Current opportunities for consumers to bring proceedings against digital health providers are limited, expensive and time-consuming with limited potential benefit in terms of compensation by the end of the process. However, once Member States have applied the measures of the Directive on representative actions, this is likely to greatly increase the enforcement of consumer rights across the EU. For example, if a wearable product has safety issues under the General Product Safety Directive 2001/95/EC (GPSD) and a large number of consumers complain to a qualified entity, it will be able to bring a collective action against the manufacturer for alleged infringements of the GPSD. In some instances, qualified entities will be able to bring a joint representative action along with consumer protection groups and NGOs from other Member States if there is an EU-wide issue.

Injunctions and consumer redress

Qualified entities will also be able to apply for injunctive relief and other redress with injunctions potentially being granted on a preventative or prohibitive basis. In addition, qualified entities may seek redress on behalf of consumers in the form of compensation, repair, replacement, price reduction, contract termination or reimbursement. The redress awarded could vary among consumers in the group or could be the same for all consumers involved in the action. Member States will be given some flexibility as to how this will operate and be able to decide to:

- Opt-in, i.e. consumers actively opt-in to being represented, or
- Opt-out, i.e. a consumer must express their desire not to be represented by a qualified entity, mechanism

For cross-border actions, only the opt-in basis will be available.

Safeguards

One of the important features of the Directive on representative actions are the safeguards which were introduced in order to ensure the system does not encourage frivolous lawsuits. These include:

- Loser pays principle: The costs of the proceedings should be borne by the unsuccessful party
- Dismissal of manifestly unfounded cases: Courts will also be willing to dismiss manifestly unfounded cases at the earliest possible stage of the proceedings
- Potential for settlement: There is also the possibility that a claim can be settled. However, such a settlement requires the approval of the court
- Third party funding: A qualified entity will be required to publicly disclose information about its sources of funding for the representative actions it brings. At present, third party funding in Ireland is prohibited

- Multiple claims by individual consumers: Member States will be required to lay down rules preventing consumers from bringing an individual action or being involved in another collective action against the same trader for the same infringement. Furthermore, Member States must ensure that consumers do not receive compensation more than once for the same cause of action against the same trader

The way forward

Member States will be required to adopt implementing measures by 25 December 2022 and the measures will apply from 25 June 2023. While it remains to be seen how it will be implemented in practice, Digital Health businesses should begin to prepare for an inevitable increase in litigation and the introduction of cross-border collective actions will be a particular interest for businesses with a presence in multiple Member States.

Draft Proposal for the Regulation of Ethical AI

Brian McElligott
Partner,
Intellectual Property & AI
bmcelligott@mhc.ie

On 20 October 2020, the EU Parliament approved an initial draft proposal for the regulation of ethical artificial intelligence (AI). The proposal targets high risk AI in particular, but also sets standards for all AI products and applications. The scope of application of the proposal is very broad in that it covers all uses of AI products in the EU regardless of the origin or place of establishment of the developer or owner of the AI. It also regulates not only the developers of AI, but also the deployers and users of those AI products and applications.

The proposal is in the form of a Regulation which means that it should be binding in its entirety and directly applicable in Member States. There are frequent references, however, to rules, guidelines and applications that are to be developed on foot of the Regulation.

What will be regulated?

The Regulation applies to "artificial intelligence", "robotics" and "related technologies", including software, algorithms and data used or produced by such technologies, developed, deployed or used in the Union.

Each of artificial intelligence, robotics and related technologies are defined terms and broadly cover:

- AI software/hardware systems (artificial intelligence)
- Physical machines with AI capability (robotics), and
- Other technologies such as those capable of detecting biometric, genetic or other data (related technologies)

High risk AI

Article 5 of the Regulation sets the minimum compliance threshold for all AI. AI shall be developed, deployed and used in the Union in accordance with Union law and in full respect of human dignity, autonomy and safety, as well as other fundamental rights set out in the EU Charter of Fundamental Rights.

Articles 6 - 12 and 14 deal specifically with high risk AI. These are technologies when their development, deployment or use entails a significant risk to cause injury or harm that can be expected to occur to individuals or society in breach of fundamental rights and safety rules, as laid down in Union law.

This is determined following a risk assessment based on objective criteria such as their specific use or purpose, the sector where they are developed, deployed or used and the severity of the possible injury or harm caused.

High risk AI must comply with obligations, such as:

1. A guarantee of full human oversight at any time, including in a manner that allows full human control to be regained when needed, including through the altering or halting of those technologies
2. Assurances of compliance with minimum cybersecurity baselines proportionate to identified risk, reliable performance, accuracy, explainability, disclosure of limitations and the provision of a form of kill switch
3. A lack of bias and that it will not discriminate on grounds such as race, gender, sexual orientation, pregnancy, national minority, ethnicity or social origin, civil or economic status or criminal record
4. Compliance with relevant Union law, principles and values in a manner that does not interfere in elections or contribute to the dissemination of disinformation, respects workers' rights, promotes quality education and digital literacy, does not increase the gender gap by preventing equal opportunities for all and does not disrespect intellectual property rights
5. Environmental sustainability ensuring that measures are put in place to mitigate and remedy their general impact as regards natural resources, energy consumption, waste production, carbon footprint, climate change emergency and environmental degradation in order to ensure compliance with the applicable Union or national law, as well as any other international environmental commitments the Union has undertaken
6. Very tight restrictions for any use of biometric data for remote identification purposes in public areas, such as biometric or facial recognition

Redress

Any natural or legal person shall have the right to seek redress for injury or harm caused by the development, deployment and use of high-risk AI, robotics and related technologies, including software, algorithms and data used or produced by such technologies, in breach of Union law and the obligations set out in this Regulation. The scope of this proposed right will no doubt concern all AI product developers and deployers.

Risk assessment and supervisory authorities

The proposal envisages mandatory compliance assessments for high-risk AI and voluntary certificates of ethical compliance for all other AI. The process of certification is to be carried out locally at Member State level by supervisory authorities. This approach is very similar to the current regulation of data protection under the GDPR. There will be an overarching group of supervisory authorities that will meet at EU level with the Commission to oversee the operation of the certification and monitoring of AI. It is not made clear in the proposal if the mandatory compliance assessments are pre-market launch.

Annex

The Annex to the draft contains specific and exhaustive lists of high-risk AI sectors and high-risk uses or purposes of AI which will always be regulated. The high-risk sectors are:

- Employment
- Education
- Healthcare
- Transport
- Energy
- Public sector (asylum, migration, border controls, judiciary and social security services)
- Defense and security, and
- Finance, banking, insurance

The high-risk uses or purposes are:

- Recruitment
- Grading and assessment of students
- Allocation of public funds
- Granting loans
- Trading, brokering, taxation, etc.
- Medical treatments and procedures
- Electoral processes and political campaigns
- Public sector decisions that have a significant and direct impact on the rights and obligations of natural or legal persons
- Automated driving
- Traffic management
- Autonomous military systems
- Energy production and distribution
- Waste management, and
- Emissions control

The draft proposal broadly follows the findings of the Commission's White Paper from earlier in 2020. However, the scope of the obligations and high-risk sectors and uses is a lot broader than expected. The fact that deployers and users are mostly regulated in the same way as developers is also a change but not an unexpected one, having regard to recent lobbying activities.

This is an early draft of this very important law and it will prove very challenging for those developing and deploying high-risk AI. We can expect significant debate on the drafting before we see a fully formed proposal early this year.

AI Laws & Timelines

10 April 2018

Member States sign up to cooperate on AI

1 June 2018

AI high level expert group (HLEG) appointed & AI Alliance launched

7 June 2018

Horizon Europe programme proposed: largest EU R&I programme ever with €100 billion

7 December 2018

Coordinated plan with Member States: boost AI made in Europe. All EU countries to develop own AI strategies by mid-2019

18 December 2018

Consultation on draft ethics guidelines by AI HLEG

8 April 2019

Commission presents approach to build trust in human-centric AI

9 April 2019

Digital Day Presentation and discussions on AI ethics guidelines

26 June 2019

Policy & investment recommendations by AI HLEG. Pilot phase of AI ethics guidelines

19 February 2020

European Commission publishes White Paper aiming to foster a European ecosystem of excellence and trust in AI and a Report on the safety and liability aspects of AI

14 June 2020

End of public consultation on White paper and Report on liability

23 July 2020

Beginning of Inception Impact Assessment

20 October 2020

Publication of draft proposals for rules for AI

Q1 2021

Expected draft legislation

Brexit Considerations for Digital Health Companies

James Gallagher
Senior Associate,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Introduction

As the process of learning to operate in the actual "post-Brexit" world begins in earnest, digital health companies must now stay up to speed with a diverging regulatory regime in the UK while also preparing for changes in the way software products are regulated as medical devices at European level. While new UK Brexit legislation continues to come into force and guidance on its operation continues to evolve, organisations competing in the digital health space need the clearest possible understanding of where we are in the Brexit process and what is yet to come. As we enter 2021, there are a number of key changes to be aware of.

Key changes

The transitional period where EU law continued to apply to the UK as an EU Member State ended at 11pm (GMT) on 31 December 2020. A number of regulatory changes have now officially come into force and are part of a new way of doing business.

Distributors and importers

Under EU law, a "third country" is a country outside of the EU and therefore the UK is now a third country. EU distributors of products received from manufacturers or importers established in the UK may now themselves be importers of those goods. As a result, they may be subject to more stringent obligations in terms of ensuring that the products they are importing from a third country (the UK) comply with EU requirements.

Notified Bodies

EU legislation provides for Notified Bodies, which must be established in a Member State and designated by a Member State competent authority, to take part in the conformity assessment procedure for certain types and classes of medical device. UK-based Notified Bodies have now lost their status as Notified Bodies and can no longer perform conformity assessment tasks to enable products to acquire valid certification for placement on the EU market. If a device has previously obtained its EU certification using a UK-based Notified Body, that certificate is no longer valid.

The opportunity to begin the process of transferring the certificate to a EU-based Notified Body has now passed, and an application for a new certificate issued by a EU-based Notified Body needs to be made.

MHRA registration

There is now a requirement to register all medical devices, including software medical devices placed on the UK market and most medical devices placed on the Northern Irish market, with the Medicines and Healthcare products Regulatory Agency (MHRA). There are a set of grace periods to allow compliance with this new process that are linked to the type and class of device in question:

- Class III medical devices, Class IIb implantable medical devices, active implantable medical devices and IVD List A must be registered from 1 May 2021
- Class IIb non-implantable medical devices, Class IIa medical devices, IVD List B and self-test IVDs must be registered from 1 September 2021, and
- Class I medical devices and general IVDs must be registered from 1 January 2022

Authorised Representatives

Device manufacturers with a registered place of business outside the EU must have an "authorised representative" that is established within the EU to act on their behalf in carrying out certain tasks when placing devices on the EU market. From 1 January 2021, authorised representatives established in the UK (other than Northern Ireland) are no longer recognised. As a result, manufacturers that previously used a UK (other than Northern Ireland) based authorised representative must now designate a UK Responsible Person when placing devices on the UK market (other than Northern Ireland). Accordingly, they must designate an authorised representative established in a Member State or Northern Ireland when placing devices on the EU market.

UK Responsible Person

Device manufacturers established outside of the UK must now also have a UK Responsible Person (RP) to register devices with the MHRA and act on their behalf in respect of devices placed on the UK market. Current MHRA Guidance for the UK market (other than Northern Ireland) provides that manufacturers should appoint their RP *"as soon as possible, where required"*. MHRA guidance for the Northern Irish market states that *"manufacturers must appoint a UK Responsible Person before they can place their device on the Northern Ireland market"*. There are no specific requirements for qualifications or knowledge for the position, but the RP must be competent to carry out their responsibilities and must be physically located in the UK.

UK Conformity Assessment Procedure

The UK Conformity Assessed (UKCA) marking is now the UK mark required for devices placed on the UK market that used to require a CE mark. All devices placed on the UK market, other than Northern Ireland, will be required to be certified under the UKCA marking from 1 July 2023. Northern Ireland will retain a system that uses the CE marking in combination with a new UK(NI) marking. Where required, designated UK Notified Bodies are now known as "Approved Bodies" and are the UK Conformity Assessment Bodies for the purposes of conducting assessments against UK requirements for the purpose of the UKCA mark. The UKCA marking will not be recognised in the EU market, and devices manufactured in the UK for placement on the EU market will still need a CE mark.

Customs

The UK is now no longer a member of the EU Customs Union. As a result, customs procedures required under EU law now apply to all goods entering the EU customs territory from the UK, other than Northern Ireland, or leaving the EU customs territory to the UK, other than Northern Ireland. Additional controls will now need be carried out as part of customs protocols that apply to all goods entering the EU from outside its borders. Although this might not have an immediate impact in the case of software products, these controls are likely to lead to increased administrative pressures on supply chains carrying hardware and other physical components that function in tandem with Digital Health solutions.

Northern Ireland

Rules for placing medical devices on the Northern Irish market from 1 January 2021 differ from those applicable to the rest of the UK in certain respects. Some of these rule changes include:

- The MDR and IVDR will apply in Northern Ireland from 26 May 2021 and 26 May 2022 respectively
- The CE marking will continue to be required and in addition, the new UK(NI) marking will be required if a UK Notified Body undertakes mandatory third-party conformity assessment
- Certain devices placed on the Northern Irish market need to be registered with the MHRA from 1 January 2021. However, there are also certain grace periods in place that are linked to the type and class of device in question
- The requirement to appoint a UK-based RP for the purposes of the Northern Ireland market will not apply where a third country manufacturer has an Authorised Representative based in Northern Ireland. Third country manufacturers who do not have an Authorised Representative based in Northern Ireland are required to have a RP appointed from 1 January 2021 for devices that are placed on the Northern Irish market
- Conversely, Great Britain manufacturers will be required to appoint an Authorised Representative based in the EU or Northern Ireland in order to place a device on the Northern Irish (and EU) market
- In cases where the Northern Irish importer is not the Northern Ireland-based Authorised Representative or the UK-based RP, the importer will be required to inform the relevant Northern Ireland-based Authorised Representative or the UK-based RP of their intention to import a device. In such cases, the Northern Ireland-based Authorised Representative or the UK-based RP will be required to provide the MHRA with a list of device importers

Conclusion

2021 promises to be a busy year for digital health companies working to make their innovative solutions available to consumers throughout the EU, the UK and Northern Ireland. Although these diverging regimes have the potential to frustrate existing timelines and delay launches, the indications are that with careful monitoring and detailed planning, the disruptive impact of Brexit will hopefully do little to slow the rolling out of ever more life-changing and life-improving technologies for patients and consumers throughout the European, British and Northern Irish markets.

Proposed Digital Services Act: A Changing Liability Regime for Service Providers

John Farrell
Partner,
Commercial & Technology
jfarrell@mhc.ie

Introduction

The European Commission published the draft text of the Digital Services Act (DSA) on 15 December 2020. It is intended to reflect the significantly changed landscape since the E-Commerce Directive 2000/31/EC (E-Commerce Directive) was enacted 20 years ago. The DSA will be implemented as an EU Regulation and will largely uphold the current liability regime under the E-Commerce Directive. Like many other key legislative reforms in the Digital Single Economy over the past few years, the DSA will apply where recipients of services are based in the EU, regardless of the service provider's place of establishment. It contains new obligations in relation to digital services that connect consumers to goods, services and content, as well as new procedures for faster removal of illegal content and measures for protecting users' fundamental rights online.

Specific measures for intermediary services

There are provisions set out for intermediary service providers of:

- A mere conduit service
- A caching service, or
- A hosting service (in order to avoid liability for illegal content where certain specified conditions are met)

Providers of intermediary services based outside of the EU will be required to designate a single point of contact to communicate with Member State authorities. There will also be reporting obligations for removal and disabling information which is illegal or contrary to providers' terms and conditions, as well as mechanisms to allow third parties to notify of the presence of illegal content.

Additional provisions for providers of hosting services

Content moderation also comes in to focus, and there are notice and action mechanisms. A statement of reasons will need to be issued to recipients where a service provider removes or disables access to items.

Additional provisions which apply to all online platforms

There is a specific exception for micro or small enterprises, which are those that employ fewer than 50 persons and whose annual turnover does not exceed €10 million.

All other online platforms will be required to have an internal complaint-handling system to make decisions about illegal content or information violating the provider's terms and conditions. In the event of a dispute, online platforms are required to engage in and inform complainants of the possibility of using an out-of-court settlement process. This will involve independent bodies in the relevant Member State reviewing the decisions of online platforms to take down content. Trusted flaggers, entities who are experts at reporting illegal content, may submit notices of illegal content as part of a notice and action procedure. The platform must then process and decide upon it with priority and without delay. In order to be awarded trusted flagger status by the Digital Services Coordinator of a Member State, the applicant will need to meet the following conditions:

- It has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content, and
- It represents collective interests and is independent from any online platform; and it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner

The Digital Services Coordinator will revoke the status of the trusted flagger if it determines, following an investigation, that the entity no longer meets the criteria set out above.

Specific 'know your business customer' obligations will apply to online platforms regarding the traders on their platform. The aim is to ensure a safe, transparent and trustworthy environment for consumers and to discourage traders who sell unsafe or counterfeit goods. Traders will be required to submit proof of identification and self-certify to only offer products and services that comply with applicable EU laws. Online platforms will be required to keep information about the traders to help trace sellers of illegal goods or services.

Online platforms will have to make reasonable efforts to assess the reliability of certain traceability information. They should:

- Appoint a single point of contact in the EU
- Appoint a legal representative in the EU
- Include information on any restrictions on use of the services in terms and conditions
- Submit detailed reports at least once a year on content moderation

In addition, the DSA also requires online advertising transparency. Online platforms must give users immediate information on the sources of the advertisements they see online, including information on why an individual has been targeted with a specific advertisement. The liability safe harbour provisions are expressly excluded for online platforms where illegal content is presented in a way that creates the impression that such content is provided by the platform itself or under its control.

Online platforms are required to notify an enforcement authority on suspicion that a serious criminal activity involving a threat to the life or safety of persons has taken place, is taking place, or is likely to take place.

Very Large Online Platforms

Very large online platforms, which are those that reach 45 million users or more, will be required to:

- Carry out risk assessments on the use and functioning of their services, and
- Put mitigating measures in place to protect users from illegal content, goods and services

When such platforms recommend content, users will be able to modify the criteria used and choose not to receive personalised recommendations. Very large platforms will need to make information publicly available on:

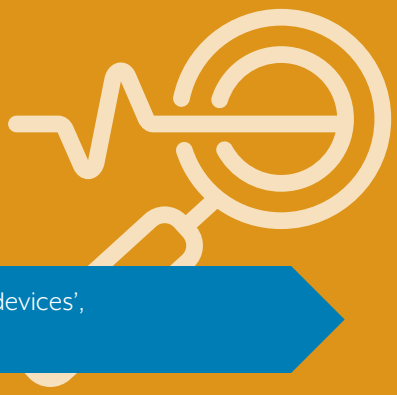
- The content of the advertisement
- The natural or legal person on whose behalf the advertisement is displayed, and
- The period during which the advertisement was displayed

This information must be retained for a year after the advertisement was last displayed on the platform.

What happens next?

The Proposed text for the DSA is still at draft stage and has yet to be discussed with the European Parliament and the European Council. While the key protections afforded by the E-commerce Directive are maintained, many organisations will no doubt be concerned around the increased reporting obligations which the DSA may introduce. This will likely receive significant discussion at EU Parliament level.

Top 10 Guidance for Digital Health 2020



1. MDCG, 'Guidance on Cybersecurity for medical devices', (December 2019)
2. The European Commission, 'White Paper on Artificial Intelligence – A European approach to excellence and trust', (February 2020)
3. The European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics', (19 February 2020)
4. MDCG, 'Guidance on significant changes regarding the transitional provision under Article 120 of the MDR with regard to devices covered by certificates according to MDD or AIMDD', (16 March 2020)
5. World Health Organization (WHO), 'Draft global strategy on digital health 2020-2024', (March 2020)
6. Data Protection Commission, 'Report by the Data Protection Commission on the use of cookies and other tracking technologies', (April 2020)
7. The European Commission, 'Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection', (April 2020)
8. MDCG, 'MDCG Position Paper on the use of the EUDAMED actor registration module and of the Single Registration Number (SRN) in the Member States', (August 2020) and the European Commission, 'Actor Module FAQs v1.1' (December 2020)
9. The European Parliament resolutions on the regulation of artificial intelligence (October 2020)
   - Framework of ethical aspects of artificial intelligence, robotics and related technologies
   - Civil liability regime for artificial intelligence
   - Intellectual property rights for the development of artificial intelligence technologies
10. MDCG, 'Questions and Answers related to MDCG 2020-4: "Guidance on temporary extraordinary measures related to medical device notified body audit: during COVID-19 quarantine orders and travel restrictions"' (December 2020).

Data Protection & Digital Health in 2020: Balancing COVID-19 & Privacy

Brian Johnston
Partner,
Privacy & Data Security
bjohnston@mhc.ie

Introduction

As part of the battle against COVID-19, various significant measures have been introduced throughout the EU that have resulted in a significant increase in the collection of data relating to individuals' health, location and social habits. Examples of such measures include the contact tracing apps developed by EU Member States to track and trace the transmission of COVID-19, the obligations on businesses to collect and retain details of customers entering their premises and employers implementing temperature screenings.

While combatting the virus is of paramount importance, these measures impact on individuals' data protection rights and ensuring these rights are protected is also a critical consideration, as illustrated by statements from the European Data Protection Board and others throughout 2020.

For anyone collecting such information, there are a number of key principles to bear in mind:

- **Transparency:** adopt a "no surprises" policy. Be clear with individuals about what information is being collected, for what purposes, who it will be shared with and how long it will be retained
- **Data minimisation:** only collect the information you need. Don't collect information because you think it might be useful or valuable at a later date. Holding information you don't need only create unnecessary risk – especially where it is sensitive and related to COVID-19
- **Purpose limitation:** only use information for the purpose for which you have collected it. For example, if you collect information for contact tracing purposes don't use it for marketing purposes later. Customers won't thank you for it and it could draw the attention of data protection regulators
- **Retention:** once you no longer need data, such as to comply with legal obligations or retention requirements, you should delete it. It should not be kept "just in case"
- **Security:** much of the information will be highly sensitive for those to whom it relates and so extra care should be taken when storing it. Ensure appropriate security measures are in place, regular reviews are undertaken of the measures and ensure that access to the information is restricted to a "need to know" basis only

An EU Approach to health data

While the EU Commission has strived for uniformity of rules regarding the processing of personal data in the EU, there continues to be significant disparity at Member State level regarding the use of health data. For example, any organisation seeking to conduct health research throughout the EU will be aware of the different rules and processes that need to be followed and the challenges such disparity can cause.

The COVID-19 pandemic has underlined the key role that technology can play in improving public health and the importance of utilising health data to achieve those objectives – and how disparity in Member State rules in approaches can stifle progress in this area.

In response to this, the EU Commission announced in November 2020 its intention to work on a secure and patient-oriented use of health data for Europe. It also announced an EU-wide collaboration in this area, through a "European Health Data Space" for better healthcare, better research and better health policy making. The EU Commission considers that a common European Health Data Space will promote better exchange and access to different types of health data such as electronic health records, genomics data, data from patient registries etc. This would not only support healthcare delivery (primary use of data) but also for health research and health policy making purposes (secondary use of data).

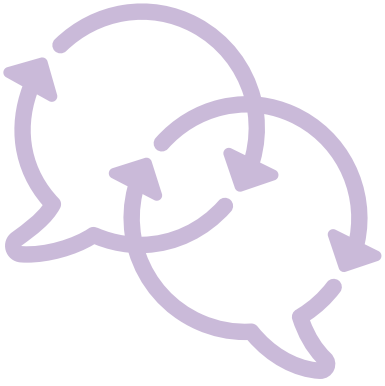
We can expect to see further significant developments in this area in the coming months and years as the EU looks to unlock the benefits of this EU-wide approach to health data.

Brexit and the free flow of data

One of the few good news stories of 2020 – at least from a data protection perspective – was the Brexit Trade Deal, which was agreed on 24 December 2020.

While the UK did not secure an "adequacy decision" from the EU Commission as it had hoped, the deal provides that on an interim basis the UK will not be treated as a "third country" for the purposes of GDPR and data transfers, as many had feared. This is hugely positive for those transferring data from the EU to the UK. In practice it means that transfers can continue to take place seamlessly between the EU and the UK, as was the case pre-Brexit, and there is no need for companies to put in place transfer mechanisms, such as the EU Commission approved Standard Contractual Clauses.

This is only an interim position and it will need to be reviewed again by mid-2021 at the latest. However, there is cause for some optimism that the UK will secure an adequacy decision from the EU Commission during that intervening period and ensure there can continue to be a free flow of data between the UK and EU. This will be a key issue to watch for those doing business in the UK.



Guidance Update: Medical Devices Regulation Article 120

Eithne Barry
Associate,
Product Regulatory & Liability
ebarry@mhc.ie

Introduction

In March 2020, the Medical Device Coordination Group (MDCG) published two guidance documents in relation to Article 120 of the MDR. Article 120(3) is of significance to certain manufacturers of Class I devices under the Medical Device Directive (MDD) that may, if certain criteria are met, remain on the market under their MDD certificate until 26 May 2024.

Class I transitional provisions

MDCG 2020-2: Class I Transitional provisions under Article 120 (3 and 4) – (MDR) – March 2020 (MDCG 2020-2) clarifies that to make use of Article 120(3) of the MDR, the following conditions must be met:

1. The device continues to comply with the MDD
2. A notified body will need to be involved under the MDR
3. A valid Declaration of Conformity, according to Annex VII of the MDD, must be drawn up before 26 May 2021
4. No significant changes to the design or intended purpose of the device after 26 May 2021. Guidance under MDCG 2020-3 clarifies what must be considered a significant change within the meaning of Article 120 of the MDR, and
5. The requirements of the MDR relating to post-market surveillance, market surveillance, vigilance, registration of economic operators and of devices shall apply in place of the corresponding requirements in the MDD. This shall be in place from 26 May 2021

MDCG 2020-2 also provides specific further guidance in relation to point (3) above and sets out how the Declaration of Conformity, which is to be prepared by the manufacturer, is to be drawn up.

Significant Changes

MDCG 2020-3: Guidance on significant changes regarding the transitional provision under Article 120 of the MDR with regard to devices covered by certificates according to MDD or Active Implantable Medical Devices Directive (AIMDD) – March 2020 (MDCG 2020-3) provides a roadmap of different assessment steps which can be taken to determine when a change should be deemed "significant" or not.

Manufacturers themselves can assess their proposed change against various flowcharts in the Guidance to determine whether or not this would render the change "significant":

- **Chart A** relates to changes to the intended purpose of the device. Examples of significant change include new user or patient population, change of clinical use, new anatomical site or an extension of the intended purpose
- **Chart B** relates to changes affecting the design performance specification. Significant changes would include changing operating sources, adding new clinical data to support, changing the source of energy or alarms and adding new risks that require control measures
- **Chart C** deals with changes to software. Significant changes under this category would include new or major changes to the operating system, new user interface, new diagnostic features or new channels of inter-operability, user input replaced with closed loop algorithm, modified architecture or database structures, algorithm and major changes to the operating system
- **Chart D** considers changes in material. Significant changes within this category would include changes with regard to human/animal origin, ingredients from a new supplier with new specifications and medicinal substances impacted by the change
- **Chart E** discusses changes with regard to sterilization or packaging design that impacts sterilization. A change would be ruled significant under this category whereby the new package design impacts sterilization, an extension of expiry without prior Notified Body review of methodology, new sterilization method or a design change which impacts sterilization

For Class I medical devices requiring the involvement of a Notified Body for the first time, manufacturers of these devices must be able to justify their decision when the changes are considered non-significant. No administrative changes are to be considered as significant. This includes changes of the manufacturer's name, address, legal form or changes of the authorised representative.

Although most of the guidance focuses on changes to the device, materials, or its intended purpose, those are not the only changes a Notified Body may rule significant enough to invalidate an MDD CE certification and thereby end the transitional period the manufacturer hoped to benefit from. Quality Management System (QMS) changes may also be considered significant. These include changes in company ownership, new facility or line modification/relocation, post-market surveillance and vigilance issues, changes in authority of the management representative and concerns about implementation or corrective actions.

Conclusion

The window for manufacturers to renew existing or obtain new MDD certificates remains open. Availing devices that satisfy the relevant criteria can be placed on the market up to May 2024 and be made available to end-users up to May 2025. This will allow manufactures to continue to supply their medical devices whilst also preparing for eventual up-classification under the MDR. However, understanding what will be deemed "significant" is critical before implementing a change, and the guidance should be considered carefully as a result.

A Civil Liability Regime for Artificial Intelligence

Michaela Herron
Partner,
Product Regulatory & Liability
mherron@mhc.ie

Introduction

A report, which sets out the recommendations of members of the European Parliament to the European Commission on how artificial intelligence (AI) should be regulated in the area of civil liability, was adopted by the European Parliament on 20 October 2020 (the Report). It is hoped that the Report will influence the Commission's forthcoming legislative proposals in the realm of AI regulation. The Report also contains the draft text of a proposal for a Regulation on the civil liability regime for AI.

Who should be liable?

- The Report proposes a new regime for civil liability claims of natural and legal persons against so-called "Operators" of AI systems
- The Report considers that in situations where there is more than one Operator, all Operators should be jointly and severally liable, while having the right to recourse proportionately against each other

Review of the Product Liability Directive and General Safety Framework

- The Report urges the Commission to assess whether the Product Liability Directive 85/374/EEC should be transformed into a Regulation. It also seeks clarification of the definition of "products" by determining whether digital content and digital services fall under its scope
- It also calls on the Commission to consider adapting concepts such as "damage", "defect" and "producer", and to consider whether the concept of "producer" should incorporate manufacturers, developers, programmers, and other service providers
- The concept of "time when the product was put into circulation" was also considered in the Report. It calls on the Commission to assess possible adjustments to the EU safety framework, in particular whether the concept is fit for purpose for emerging digital technologies, and whether the responsibility and liability of producers could go beyond this, taking into account that AI-driven products under the producer's control may be changed or altered after they have been placed on the market,

which could cause a defect and ensuing damage. This concept has always been to the forefront when considering product liability and AI. From the perspective of certainty, this could be a welcome change for Operators

High-risk AI systems

- One of the most significant features of the Report is the regime of strict liability imposed on Operators of high-risk AI systems. This provides that they will be strictly liable for any harm or damage that was caused by a physical or virtual activity, device or process driven by that AI system. This means that Operators of high-risk AI-systems will be liable for any harm caused by an autonomous activity, device or process driven by their AI system, even if they did not act negligently
- The Report defines a high risk as meaning "significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected, the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used"
- The Report proposes that all high-risk AI systems be exhaustively listed in an Annex to the proposed regulation, and that they be reviewed at least every six months and updated if necessary via a delegated act. This should provide clarity in categorising high-risk AI systems, and this is necessary as the consequences of classification are significant

Compensation and limitation periods for high-risk AI systems

- In terms of compensation, the Report proposes that there should be a maximum compensation of €2 million payable in case of death or harm to a person's physical health or integrity resulting from an operation of a high-risk AI-system and a maximum of €1 million in the case of significant immaterial harm (economic loss or damage to property)
- The Report proposes lengthy limitation periods, allowing claims to be brought up to 30 years after the event. The Report proposes 30 years for claims concerning harm to life, health or physical integrity and 10 years in case of property damage or significant immaterial harm that results in a verifiable economic loss
- These are very lengthy limitation periods and far greater than those provided for under the Product Liability Directive 85/374/EEC

Conclusion

The current proposal would require providers of AI systems to check whether they fulfil the definition of "Operator" and undertake a risk assessment of their technology. As we have seen, the Report suggests imposing strict liability on those operating high-risk AI if there is damage caused. Therefore the classification of AI systems will be a crucial point of consideration for Operators.

A robust civil liability framework for AI may present challenges to businesses in its implementation but it should also provide legal certainty, protect citizens better and enhance their trust in AI technologies by deterring high-risk activities. In this respect, the Report is welcomed and we await feedback from the European Commission on how the proposal will be taken forward. It is also anticipated that a number of these issues will be carefully considered during the European Commission's upcoming review of the Product Liability Directive 85/374/EEC and the General Product Safety Directive 2001/95/EC.

Irish Fundraising Trends for Digital Health Businesses

Robert Dickson
Partner,
Corporate
rdickson@mhc.ie

Introduction

During 2020 we saw considerable continued investor appetite to partake in funding rounds for digital health businesses. Some recent rounds have been of significant size. As other sectors of the market have been challenged, venture capital and private equity investors have sought to deploy their capital in sectors with major growth potential. As consumers become increasingly familiar with the concept of managing their health remotely through digital platforms, digital health businesses have increased their market share. This means the opportunities and value of businesses in the digital health sector has been recognised by investors through large investments, hence the significant deal volume in the sector. If you are an investor considering investing in an Irish company owning a digital health business, or you are a digital health company raising equity funding, it is important to be aware of some deal trends in the Irish market.

Investor geography

When Irish businesses are raising investment, that investment tends to come from a range of international geographies, as well as from Irish investment houses. The most typical geography of an investor in investment transactions we advise on is the US. This is far more prevalent than investments by Irish-based investors, which would be the second most common investor geography on our transactions. Investment by US private equity and venture capital investors into growing Irish digital health businesses is something we regularly encounter, especially on the larger investment rounds.

Exit rights

A private equity or venture capital investor will always be focused on its exit and the value of its return on its investment. The deal documents will always include various rights and obligations setting out the extent to which an investor will have the right to trigger an exit process, or even a hard right of sale at a given value if the exit process fails. The latter is much less common and tends to only be capable of being invoked in very specialised circumstances.

Sale rights and protections

Drag along rights are a standard feature of Irish shareholders' agreements or constitutions. Tag along rights, pre-emption rights on transfer of shares, and pre-emption rights on allotment of shares are also usually included. The question with many of these deal terms is not whether they are included, but the nuances within the relevant clauses. For instance, it is important to consider carefully which shareholders are to be capable of dragging others into a sale. Also, although pre-emption rights on transfer are a useful protection for shareholders in a company, it is important to consider whether shareholders are permitted to sell their shares at all, or whether "lock-in" restrictions should be included.

Secondary element to fundraising

In a minority of the equity investment deals we advise on, the investors acquire some shares from the existing shareholders, as well as investing new money into the business for its working capital in exchange for new shares in the business. We tend to see existing shares being sold as part of these transactions in some private equity deals rather than venture capital deals. This only tends to happen in businesses that are throwing off considerable revenue, rather than in other fast growth, high value, but low revenue businesses. However, in the right circumstances, this can be a really positive deal term for investors and founders alike, which can be very popular with private equity investors as a way of bringing out the best long-term performance from management.

Anti-dilution rights

It is more common than not to include anti-dilution rights in Irish investment deal documents. This gives investors comfort that if there is a subsequent "down round", the investor will be made whole on its percentage shareholding in a subsequent exit.

Warranties

It is typical for a long-form suite of warranties to be provided by the investee company to the investor(s) in an Irish Investment Agreement. These still tend to be capped at the full investment amount – which is quite different to M&A trends, in which we are increasingly seeing lower percentage caps as against the consideration amount. More often than not, those warranties are supplemented by further warranties from a member of the founder or management team. This tends to be capped at a low multiple of that individual's salary. We see anything from 1x to 3x, or another agreed six-figure sum. On some smaller investment rounds prior to Series A stage, we sometimes see a shorter form set of warranties, usually 4-5 pages.

Indemnities

As well as the typical suite of warranties typically observed in Irish transactions, specific indemnities are usually provided by the sellers in M&A transactions, relating to specific known risks which are uncovered by the due diligence process. Conversely, it is extremely unusual for specific indemnities to be included in investment transactions. This is due to the nature of the transactions. Sellers are not exiting the business with significant sums of money and any sort of claim by an investor under the warranties or indemnities following an investment transaction is highly unusual. This is because, as part-owners of the business once their investment has been made, such an investor would consider a claim to be partially against itself. When investing in fast growth businesses in particular, investors typically accept that there will be risks and matters to be perfected, and do not usually escalate those matters to an indemnity item as a buyer typically would in an M&A transaction.

Data room disclosure

We expect to see a Data Room produced by the investee company and its advisors, as part of the due diligence process on investment transactions. A question that sometimes arises is whether the Data Room is to be generally disclosed in the Disclosure Letter. This means that any matter which has been included in a document in the Data Room, which is clear and fair so that a reasonable investor could assess the nature of the matter or risk, will be deemed to be an exception to each of the warranties. In Irish transactions – both M&A and investment transactions – we find that it is highly unusual for the Data Room to be generally disclosed in the Disclosure Letter. However, there will be competitive situations, particularly auctions, where competitive tension can be used to ensure that an investee or seller-friendly term of this nature is added into the deal.

Deal documents

In Ireland, we do not use an "industry standard" investment agreement as the starting point on investment transactions in Ireland. However, the same documents which were used on the prior round of investment into a given business, tend to be used as a starting point on the next round of investment into that business. What this means is that the negotiations on the deal documents themselves do not always take as long as can be the case where the documents are being produced and negotiated from scratch. This can assist in closing a round of funding relatively quickly, and means that the deal terms on investment transactions can often be agreed quicker than can be the case in M&A deals.

Conclusion

In conclusion, while the volume of corporate transactions in some sectors of the market decreased in 2020, that was certainly not the case in the digital health sector. The Irish transaction market was buoyant. When approaching a transaction of this nature, it is important to assess the deal terms that you want included in the documents, and to understand market trends for transactions of this nature in the Irish market. Should you have any queries about any of the above issues or about any aspect of doing a corporate transaction in the Irish market, please contact a member of our Corporate team.

Webinars & Recent Publications

Webinars

- Software as a Medical Device (October 2020)
- Commercial Contracts – What's Market? (July 2020)
- The EU Regulation of Wearables – A Changing Landscape (July 2020)
- AI Regulation: The EU Approach (June 2020)
- Selling Online – Consumer Protection Overhaul (May 2020)
- Smart Contracts – Does Irish law have the IQ to recognise them? (May 2020)
- In-House Counsel Masterclass – Recent Developments in IP and AI (May 2020)
- Commercial Contracts During COVID-19: Onboarding, Managing and Exiting (April 2020)

Publications

- Draft Proposal for the Regulation of Ethical AI (November 2020)
- AI Overview (October 2020)
- Product Regulatory Update: Post Market Surveillance Obligations Under the MDR (September 2020)
- Manufacturers of Class I Medical Devices: Making the Most of MDR's Transitional Provisions (September 2020)
- Article 120 of the Medical Devices Regulation – When is a Change Significant? (June 2020)
- The Role of Wearables in the Battle Against COVID-19 (May 2020)
- International Publications: ICLG – Digital Health Laws and Regulations (March 2020)
- Getting the Deal Through: Product Recall in Ireland 2020
- Tough Cookie – New Guidance and Report from the DPC (May 2020)
- Complying with GDPR Timelines During COVID-19 (March 2020)
- Highlights of the Data Protection Commission's Annual Report for 2019 (February 2020)
- The Regulation of AI – What Next? (January 2020)
- Key Tech Trends in 2020 (January 2020)

About us

Mason Hayes & Curran LLP is a business law firm with 95 partners and offices in Dublin, London, New York and San Francisco.

We have significant expertise in product, privacy and commercial law, which are sectors at the forefront of Digital Health Law. We help our clients devise practical and commercially driven solutions to the complex and ever changing digital technology regulatory framework. Our approach has been honed through years of experience advising a wide range of clients in diverse sectors.

We offer an in-depth understanding of the regulatory landscape of Digital Health, with a strong industry focus. We ensure to give our clients clear explanations of complex issues, robustly defend their interests and devise practical value-adding solutions for them whenever possible.

Key contacts

Michaela Herron
Partner, Product Regulatory & Liability
+353 1 614 2878
mherron@mhc.ie

Brian McElligott
Partner, Intellectual Property & AI
+353 1 614 2199
bmcelligott@mhc.ie

Philip Nolan
Partner, Head of Commercial and Privacy & Data Security
+353 1 614 5078
pnolan@mhc.ie

Martin Kelleher
Partner, Head of Life Sciences
+353 1 614 5206
mkelleher@mhc.ie

John Farrell
Partner, Commercial & Technology
+353 1 614 2323
jfarrell@mhc.ie

Brian Johnston
Partner, Privacy & Data Security
+353 1 614 7746
bjohnston@mhc.ie

Robert Dickson
Partner, Corporate
+353 1 614 2327
rdickson@mhc.ie

Niamh Keogh
Partner, Tax
+353 1 614 5848
nkeogh@mhc.ie

What others say about us

Our Privacy & Data Security Team

The team has a "deep knowledge of Irish and European data protection law."

Chambers & Partners, 2020

Our Privacy & Data Security Team

They "have unrivalled expertise and industry knowledge in their area."

Legal 500, 2020

Our Technology & Commercial Team

"They are always quick to respond. Guidance is always pointed and practical."

Legal 500, 2020

Our Products Team

The team possesses "a competitive edge in terms of sector and practice area expertise."

Legal 500, 2020

Our Products Team

"Excellent patent litigation and product liability capabilities, particularly in the life sciences area."

Legal 500, 2020

Dublin London New York San Francisco

MHC BRIEF

Your Insights & Events Community

Join now at MHC.ie/BRIEF