AI in medical devices

QUESTIONS AND ANSWERS

DECEMBER 2024

Introduction

Technology is changing medicine before our eyes—paradoxically, largely due to the Covid-19 pandemic.

On the macro scale, this is one of the pillars for restoring the competitiveness of Europe and Poland on the global market. On the micro scale, this is happening thanks to bold companies, especially medtech and biotech companies, developing innovative solutions and bringing them to the market, creating completely new opportunities in the areas of diagnostics, treatment, and functioning of the healthcare system.

The legal environment in this area is dynamic, and legal challenges are constantly mounting, from regulatory matters (compliance with the Medical Device Regulation and the AI Act) to protection of medical data and intellectual property issues.

Instead of just citing the regulations, we decided to share a hypothetical case study showcasing how to approach the regulatory "octopus" entangling any new medtech product. We answer more than 30 questions from four key areas, but surely this does not exhaust the potential legal issues in this area.

We invite you to read our report, contact us and dialogue!

Joanna Krakowiak
attorney-at-law, partner,
life sciences and healthcare

Krzysztof Wojdyło
adwokat, partner
new technologies

Case study

The hypothetical Polish company "Medical Software" wants to launch a mobile app that uses an AI algorithm to generate advanced reports on atherosclerotic changes in blood vessels. The US-based company "Algorithmics" developed a multifunctional algorithm and then granted Medical Software an exclusive, global, fee-based licence to use the software for medical applications for the next five years, under Delaware law. Medical Software has adapted the algorithm to generate medical reports on atherosclerotic lesions.

The software must work in tandem with a physical detector—a sensor containing a micro-battery and a micro SIM card. The compatible detector was developed by the company "Smart Detectors" in cooperation with Medical Software.

The software and the detector are intended for the medical use of monitoring the functioning of carotid arteries.

Smart Detectors and Medical Software have also entered into a cooperation agreement with the owner of a well-known chain of jewellery stores, "Golden Necklace." Under the agreement, the software-compatible detector will be installed on selected, customised necklaces. Various designs and models will be available, some in gold, silver and precious stones.

The aim of the cooperation agreement is that a consumer who has purchased an **item** from Golden Necklace will be able to add on a **sensor** from Smart Detectors. With this kit, the consumer can then download an app using the AI algorithm (**software**) from Medical Software.

The software generates reports under parameters defined by the user of the necklace. New options are being added all the time. There is a fee for the reports (either a one-time fee for each report, or a monthly or annual subscription fee). The user also defines who can receive the reports. Below are examples of available types of reports and their intended recipients:

1. Report on atherosclerotic lesions. The recipient may be the user, a designated doctor, or a manufacturer of atherosclerosis drugs.
2. Stroke risk report. The report is intended for the user and the indicated doctor.
3. Report on an imminent threat to life. The recipient may be the user, a member of their family, and an emergency notification system (in which case the Medical Software server will transmit to the system the user's geolocation data, basic personal details, and telephone number for contacting

the user). In addition, the necklace can be paired with the user's vehicle. If a report of imminent threat to life is generated, the relevant information is sent to the vehicle's on-board system, which activates the emergency mode (depending on the vehicle model, the emergency mode may involve, for example, taking partial control of the vehicle by an autopilot or forcing a controlled stop of the vehicle).

The system is capable of self-improvement, i.e. the algorithm autonomously fine-tunes its parameters based on the analysed data and feedback provided by users and recipients of reports.

The software is made 60% from open-source software.

Analysis

This case study poses several questions about regulations governing medical devices, artificial intelligence, data protection, and intellectual property.

Regulations governing medical devices

1. Is the software that uses the data from the sensor a medical device?

Under the definition of a medical device in the Medical Device Regulation (Regulation (EU) 2017/745—MDR), software can be considered a medical device.

Detailed rules on treating software as a medical device in the context of the MDR definition can be found in guidance issued by the Medical Device Coordination Group (MDCG 2019-11). "Software" is defined there as "a set of instructions that processes input data and creates output data." Whether software is regarded as a medical device is determined by whether it meets all the requirements indicated in the guidance (e.g. it has a medical purpose and its purpose is to benefit individual patients).

The software in question meets these criteria, because it generates medical risk reports on an individual patient based on data from readings. Therefore, the software constitutes a medical device.

2. How to treat the detector (a hardware component) under the MDR, and how is it regulated differently from a smartwatch?

Software that is a medical device often requires a hardware component to work properly. This is also the case here.

The detector is subject to requirements under the MDR due to its medical purpose. Under the guidance on medical device software from the Medical Device Coordination Group (MDCG 2023-4), the hardware working with this software can be placed on the market as:

- An accessory to medical device software
- An integral part of a medical device (hardware and software together as one medical device), or
- A separate medical device (the hardware is a medical device and the software is a separate medical device).

In the case study here, the software and the hardware are introduced by two different companies, so it would be a natural consequence to treat them as separate medical devices.

The detector has been designed by the manufacturer for use for medical purposes. By contrast, manufacturers of popular smartwatches often emphasise that their product is for general uses of lifestyle and well-being, and not for medical applications (even if it has sensors that allow it to be used for medical purposes). Thus, in their view, the smartwatch does not qualify as a medical device.

The use intended by the manufacturer is crucial for classifying hardware as a medical device. Due to the legal definition, hardware will not be a medical device if the manufacturer's documentation and materials for users do not indicate that the hardware is intended for medical use. However, it is important to distinguish hardware from medical software, such as an EKG app for a smartwatch—the app is treated as a medical device due to its medical use foreseen by the manufacturer.

Assuming that the necklace in the case study is presented as an ornament and not as a product intended for medical use, it should not be considered a medical device, even if the manufacturer mentions its compatibility with an optional sensor, which the user can purchase separately but doesn't have to.

3. How to determine the risk class of a product under the MDR?

The MDR distinguishes four basic risk classes of medical devices, from lowest to highest: class I, class IIa, class IIb, and class III. The higher the class, the greater the risk and the more heightened the regulatory requirements. A device is assigned to a risk class according to the classification rules set out in an annex to the MDR.

According to these rules, software intended for monitoring physiological processes belongs to class IIa, except where it is intended to monitor vital

physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is placed in class IIb.

Due to the nature of the parameter tested by the device here (correct functioning of the carotid arteries), the device should be assigned to risk class IIb (a change in the tested parameter could result in immediate danger to the patient).

Similarly, the detector working with the software should be regarded as a medical device in risk class IIb. In this case, the rule that class IIb includes products specifically designed for monitoring vital physiological parameters, where the nature of variations of those parameters may cause an immediate danger to the patient, applies.

4. Is this the only risk assessment that needs to be carried out on the product?

In addition, once the Artificial Intelligence Act (Regulation (EU) 2024/1689) becomes applicable, it will be necessary to determine the risk of the product under the AI Act (see answer to question 2 in the section on the AI Act below).

5. What are the obligations under the MDR of a manufacturer placing a product on the market?

A manufacturer placing a medical device on the market is obliged, in particular, to:

- Hire a person responsible for regulatory compliance
- Prepare the necessary documentation, procedures and systems
- Perform a clinical evaluation of the device
- Assign UDI codes to medical devices, submit them to the Eudamed database (this will become obligatory in the years to come, but can be done now voluntarily), and place them on the devices
- Carry out a conformity assessment, i.e. obtain an MDR certificate issued by the notified body
- Draw up a declaration of conformity and label the products with the CE mark
- Notify the intention to place the device on the market.

6. Is it necessary to conduct clinical trials of a medical device?

Conducting a clinical trial is mandatory, with some exceptions, for implantable devices and class III devices. The product in the case study does not fall into those categories (neither the software nor the detector).

However, a clinical trial may still be necessary if there is a lack of clinical data on the device's compliance with the essential safety and efficacy requirements which the manufacturer can rely on, but instead the data must be generated.

7. Does a certification authority have to be involved?

Yes, for class IIa and IIb devices it is necessary to involve a "notified body" as part of the conformity assessment.

No involvement of a notified body is required only for class I devices (other than devices placed on the market in a sterile state, or having a measuring function, or for reusable surgical instruments).

8. Is it allowed to communicate the health functions of the product and advertise it to users (lay or professional)?

Advertising medical devices is generally permissible, but is subject to special rules under the EU's MDR and Poland's Regulation on Advertising of Medical Devices.

The product in this case is intended for use by lay persons, so it can be advertised to both professional and lay users. However, misleading advertising is banned. Advertising messages addressed to the public must also be accompanied by an appropriate warning.

9. Will it be possible to apply for reimbursement status for a product if its use will lead to savings in the healthcare system?

In Poland, modern technologies are sometimes financed from public funds (e.g. advanced robots for surgical operations).

Supporting AI technologies in healthcare is currently a subject of public debate. The Polish parliament now has a standing subcommittee on AI and transparency of algorithms (CNT015). In April 2024, the subcommittee debated the reimbursement system for use of non-pharmaceutical digital technologies employing AI, as a method for better organising the healthcare system and generally raising the quality of care delivered to society.

There are also organisations calling for development of a legal framework facilitating public financing of the use of AI in healthcare in the future.

10. Do the supervisory authorities verify the classification of the product? What are the sanctions for irregularities in marketing, sale or advertising of products?

As a rule, the manufacturer is responsible for determining the risk class, but where a notified body is involved in the conformity assessment the body will verify the classification made by the manufacturer. Under the regulations, disputes between the manufacturer and the notified body regarding product classification are resolved by the Polish regulator, i.e. the president of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products (URPL). In such cases, the regulator issues a decision determining which risk class the product belongs to.

If the product does not comply with the legal requirements, the regulator will order the manufacturer to cure the non-compliance, and if it fails to do so, the regulator may order the product withdrawn from the market. Irregularities related to the manufacturer's obligations and advertising are also subject to heavy fines of up to PLN 5,000,000.

AI regulations

1. Is the system an AI system within the meaning of the AI Act?

Under the EU's AI Act, an "AI system" is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

The definition of an AI system is notable for three features:
- The ability to make inferences (an essential feature)
- Autonomy, i.e. the ability to act to a certain extent without human involvement (an essential feature)
- Adaptiveness, i.e. the ability to learn (an optional feature).

The software in the case study here meets these characteristics:
- It processes raw data from the detector into reports with predictions and conclusions (i.e. it makes inferences)
- It generates reports without human intervention (autonomy)
- It adapts, i.e. improves itself (self-learning).

By contrast, the detector functions autonomously, but does not have the ability to make inferences. It only collects and passes on data, without analysing it or drawing conclusions. It is therefore not an AI system and is not subject to the associated restrictions.

The necklace product in the example is not subject to the requirements of the AI Act, as it does not meet the characteristics referred to in the definition of an AI system.

2. To which risk class can the system be assigned?

An AI system can be classified as a high-risk AI system because:
1. It is a product (or safety-related element of a product) listed in Annex I to the AI Act (e.g. a medical device) and is subject to conformity assessment with the participation of a notified body, or
2. It is used in an area listed in Annex III to the AI Act.

The software here should be considered a high-risk AI system based on point 1 above. This is because, first, the software is regarded as a medical device under the regulations, and second, it is subject to conformity assessment with the involvement of a notified body (see questions 1 and 7 in the MDR section). Fulfilment of these conditions means that under the AI Act, the software should be considered a high-risk AI system.

The software can also be considered a high-risk AI system based on point 2 above. This is because Annex III to the AI Act includes:

- AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics. Here, the software can be considered to display a health prompt after it determines that the user's blood vessels match the category of people at risk of stroke.
- AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage system. Here, the software can be considered to be such a system due to the functionality of assessing the patient's health in an emergency and notifying the emergency services.

Recognising that the product is a high-risk AI system listed in Annex III to the AI Act has practical implications. The AI Act differentiates the legal situation of high-risk systems from Annex I and Annex III. If a product is subject to both annexes, in our view the more restrictive standards should be applied.

3. What role can be attributed to Medical Software and Algorithmics under the AI Act?

In the situation described, it can be assumed that Algorithmics has developed a general-purpose AI model, and in connection with the Medical Software licence, it has made it available on the market, becoming a provider of a general-purpose AI model.

Because Algorithmics is a non-EU entity, it will need to appoint an authorised representative in the EU entrusted with executing EU responsibilities related to the role of provider of a general-purpose AI model. Medical Software could serve as such a representative.

Apart from providing a general-purpose AI model, it can be assumed that by adapting the algorithm to a specific role, to work with the detector and the app, Medical Software has created an AI system that it markets under its own name, for a fee. In that case, the company would be considered an AI system provider.

4. Does marketing of the software in question have to be reported?

Yes. AI systems listed in Annex III must be registered in an EU database before being placed on the market.

Because the software in question is indirectly mentioned in Annex III, it is necessary to submit registration in this case.

5. What other obligations under the AI Act arise from marketing such a system in the EU?

Under the new rules, providers of high-risk AI systems must in particular:

- Establish a risk management system
- Establish a quality management system
- Draw up technical documentation and instructions for using the AI system
- Conduct an assessment of compliance with the requirements of the AI Act (an element of the conformity assessment carried out under the MDR, conducted with the participation of the notified body assessing compliance with the MDR)
- Draw up a declaration of conformity
- Properly label the AI system (including the CE mark)
- Appropriately design the AI system (to enable human oversight, adequate accuracy, robustness and cyber security)
- Ensure that the AI system uses relevant training data
- Establish a monitoring system for the AI system after placing it on the market
- Report serious incidents related to the AI system.

6. What responsibilities and powers are involved in building and testing an AI system before it is placed on the market?

The AI Act regulates not only placing of AI systems on the market, but also construction and testing before they are introduced.

EU member states are to establish "regulatory sandboxes." A regulatory sandbox provides a controlled environment conducive to innovation, facilitating development, training, testing and validation of innovative AI systems for a limited time before they are placed on the market or deployed in accordance with a specific roadmap agreed between providers or potential providers and the competent authority.

High-risk AI systems can also be developed outside of the regulatory sandbox in real-world tests. But, for high-risk AI systems from Annex III of the AI Act, a number of conditions must be met, e.g. to prepare a test plan, obtain approval from the authority, limit the duration of tests, obtain informed consent from participants, and ensure appropriate oversight.

Regulations on protection of personal data, including medical data (GDPR)

1. Does operation of the product involve processing of personal data? If so, what kind and by whom?

Yes, operation of the product in the case study involves processing of ordinary personal data and special-category personal data.

Smart Detectors and Medical Software are involved in processing of personal data to varying degrees, and potentially so is Algorithmics (depending on whether it provides, apart from the licence, services to Medical Software that involve processing of personal data).

2. To what extent will the GDPR apply to the processing of personal data in connection with operation of the product?

The EU's General Data Protection Regulation will apply to processing of personal data in the following contexts:

- Processing of the user's "ordinary" data in connection with downloading and use of the app (data needed to create and use a profile: login, password, logs, payment data (if any), etc)
- Processing of data about the user's health in connection with operation of the product (detector + app), assuming that the detector will not work without installing the app and creating a user account
- Processing of the user's health data collected by the detector for purposes of system development
- Processing of the user's health data for creating reports and sharing them with third parties (depending on the method of sharing, i.e. whether the app is directly used for such sharing).

3. Under the GDPR, who is the controller of personal data processed in connection with operation of the product? Who bears the main obligations under the GDPR related to the product?

Type and purpose of data processing	Roles under the GDPR
Processing of the user's ordinary data in connection with download and use of the app (data needed to create and use a profile: login, password, logs, etc)	Data controller: Medical Software
Processing of the user's health data in connection with operation of the product	Data controller: Medical Software Data processor: potentially Smart Detectors; Algorithmics (depending on the arrangements between the parties and the activities they perform, e.g. if Smart Detectors has access to the data as part of the maintenance service)
Processing of health data for purposes of system development	Data controller: Medical Software (unless otherwise provided under the cooperation agreement with Algorithmics and Smart Detectors)
Processing of the user's health data for creating reports and sharing them with third parties (depending on the method of sharing)	Data controller: Medical Software Data processor: potentially Smart Detectors or Algorithmics (depending on the arrangements between the parties and the activities they perform)

4. On what basis under the GDPR can personal data be processed in connection with operation of the product, and what is the significance for data processors?

Type of data processing	Basis for processing
Processing of the user's ordinary data in connection with download and use of the app (data needed to create and use a profile: login, password, logs, etc)	Necessity of the data processing for performance of a contract with the user (Art. 6(1)(b) GDPR) Legitimate interest of the controller (Art. 6(1)(f) GDPR), e.g. in connection with claims

Processing of the user's health data in connection with operation of the product	Explicit consent (Art. 9(1)(a) GDPR) (We assume that the operation of the product cannot be regarded as conducting medical treatment.)
Processing of health data for purposes of system development	Explicit consent (Art. 9(1)(a) GDPR) The AI Act and the European Health Data Space Regulation could potentially provide additional grounds in this regard in the future.
Processing of the user's health data for creating reports and sharing them with third parties indicated by the user (depending on the method of sharing)	Explicit consent (Art. 9(1)(a) GDPR)

5. Will there be a transfer of personal data outside the EEA in connection with operation of the product? What are the consequences?

The case study does not contain information in this regard. However, if the app has to run on Algorithmics' servers in the United States, operation of the app will involve the transfer of data outside the European Economic Area. That would require a legal basis (generally either Algorithmics' signing onto the EU–US privacy framework, or adopting "standard contractual clauses").

6. Does a data protection impact assessment need to be carried out for operation of the product, and if so, by whom?

Yes, there will be grounds for arguing that a DPIA is required. The DPIA should be carried out by the controller of personal data processed by the product, i.e. Medical Software.

If an AI system is considered a high-risk AI system from Annex III of the AI Act, it will also be necessary to prepare an assessment of the impact of the AI system on fundamental rights, under Art. 27 of the AI Act.

7. Who should ensure that product users are informed about the processing of their personal data, and in what manner?

This information should be provided by the data controller, Medical Software.

For this purpose, it may for example include relevant information in the privacy policy provided when downloading, installing and using the app associated with the product (before the detector starts operating).

8. Must personal data processed in connection with operation of the product be stored in the form of medical records?

No, unless the effect of the product is tantamount to conducting medical treatment.

9. Who will be allowed to share data collected by the products with third parties, e.g. for commercial use to train the AI, and under what circumstances?

As far as non-anonymised data is concerned, it could be made available by the data controller (Medical Software), but only if it meets additional conditions, in particular:

- It first identifies the basis for processing data for this purpose, such as the user's explicit consent
- It provides users adequate information regarding the processing of their data for this purpose, and
- It carries out the relevant DPIAs.

The GDPR does not apply to data that has been anonymised (effectively and irreversibly) or aggregated data. An entity holding such data may make use of the data under general rules.

The EU's AI Act, Data Act, and EHDS Regulation have the potential to provide additional opportunities in this regard in the future.

10. Can users of the app request that Medical Software and Smart Detector provide them the data generated by the detector and the software?

To the extent that the data processed by the product constitute personal data, users will have the right to request from the data controller (in principle Medical Software) a copy of the personal data processed by the product, pursuant to Art. 15(3) GDPR. In addition, the user will be able to request the controller to provide the user with personal data concerning them which they have provided to the controller, in a structured, commonly used and machine-readable format. The need to ensure the possibility of exercising these rights should be taken into account at the product design stage.

In addition, to comply with its obligations under the Data Act, Medical Software must ensure that the product and service are designed and operate in such a way that the data from the product, including the relevant metadata necessary for interpretation and use of the data, is accessible to the user:

- By default, easily, securely, and free of charge
- In a comprehensive, structured, commonly used and machine-readable format, and
- Where appropriate and technically feasible, directly.

11. How can Medical Software obtain data to train its algorithms even before the system is released to the market?

Because the product processes health data, it can be quite challenging to acquire the actual data to train the algorithm used in the product before the system goes to market. However, the AI Act provides for some possibilities in this regard.

Art. 59 of the AI Act allows personal data lawfully collected for other purposes (not necessarily collected for training algorithms) to be used for training algorithms, within the AI regulatory sandbox, but only for the purposes of developing, training and testing certain AI systems within the regulatory sandbox, when all of the following conditions are met:

a AI systems shall be developed for safeguarding substantial public interest by a public authority or another natural or legal person and in one or more of the following areas:

i. Public safety and public health, including disease detection, diagnosis, prevention, control and treatment, and improvement of healthcare systems;
ii. A high level of protection and improvement of the quality of the environment, protection of biodiversity, protection against pollution, green transition measures, climate change mitigation and adaptation measures;
iii. Energy sustainability;
iv. Safety and resilience of transport systems and mobility, critical infrastructure and networks;
v. Efficiency and quality of public administration and public services.

b The data processed are necessary for complying with one or more of the requirements referred to in Chapter III, Section 2, of the AI Act, where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data.

c There are effective monitoring mechanisms to identify if any high risk to the rights and freedoms of data subjects, as referred to in Art. 35 GDPR and Art. 39 of Regulation (EU) 2018/1725, may arise during the sandbox experimentation, as well as response mechanisms to promptly mitigate those risks and, where necessary, stop the processing.

d Any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the prospective provider and only authorised persons have access to those data.

e Providers can further share the originally collected data only in accordance with EU data protection law; any personal data created in the sandbox cannot be shared outside the sandbox.

f Any processing of personal data in the context of the sandbox neither leads to measures or decisions affecting the data subjects, nor affects the application of their rights laid down in EU data protection law.

g Any personal data processed in the context of the sandbox are protected by means of appropriate technical and organisational measures, and deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period.

h The logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox, unless otherwise provided for by EU or national law.

i A complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation referred to in Annex IV to the AI Act.

j A short summary of the AI project developed in the sandbox, its objectives and expected results is published on the website of the competent authorities; this obligation shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

Additional options for data acquisition for algorithm training will be available to Medical Software in the future, once the EHDS Regulation comes into effect.

Intellectual property

1. What can be done to prevent competitors from launching a necklace with a similar design?

The easiest way is to apply for registration of the necklace design and obtain rights to a Community design (or national industrial design). The protection arising from registration is territorial. Thus obtaining registration of a Community design gives the proprietor protection in all countries of the European Union, while registration of a national design gives protection only in the territory of the given country.

Before registering a design, it is necessary to check the available registers to see whether an identical or similar design has previously been made available to the public (defined in the legislation as a design that does not produce a different overall impression on an informed user). Protection can only be granted to designs that meet the conditions of novelty and individual character. However, when registering a design, the office does not examine whether these conditions are met. This means that even if a design has been registered, it may not be protected, and a competitor may have the right invalidated (either in independent proceedings before the relevant office or via a counterclaim in the design protection proceedings brought against it).

Another basis for protection of the necklace design could be the Act on Copyright and Related Rights, which does not require a design to be novel at a global level, but only that it be a manifestation of individual creative activity.

The last option is protecting the design under the Unfair Competition Act (in particular Art. 13(1) and 3(1)). The Unfair Competition Act protects the economic interests of undertakings against "slavish imitation" and "passing off." To benefit from protection, the plaintiff must demonstrate market priority, and also, depending on the chosen legal basis, demonstrate that the competitor has made a nearly identical copy, or that the plaintiff's product has gained a reputation (for example, through significant expenditure on promotion and marketing of the product) and enjoys significant recognition on the market for comparable products.

2. What intellectual property clauses should be included in the joint-venture agreement between Medical Software, Smart Detectors and Golden Necklace?

Joint-venture agreements are not subject to specific regulations under the Civil Code or other Polish laws. However, such agreements are clearly admissible under the principle of freedom of contract. In the case study here, the joint-venture agreement is a tripartite agreement between Smart Detectors (co-creator of the detector), Medical Software (developer of the app and co-creator of the detector) and Golden Necklace (a jewellery company designing necklaces).

The agreement should primarily define how the parties understand the intellectual property related to the design, and who has the rights to the individual components of the necklace (e.g. copyright to the detector software and app software, and necklace designs).

The agreement must:

- Indicate what rights to use intellectual property (in practice, licences) each party grants to the other parties
- Identify the scope of use (fields of exploitation, territory, duration of the licence, e.g. only for the duration of the parties' cooperation) and restrictions.

In the case at hand, it seems crucial to ensure that the parties use the intellectual property of the other parties only in the context of this specific cooperation. They should not be able to use, let alone develop, the intellectual property of other parties outside the common project.

In joint ventures, the cooperating parties will often jointly develop improvements or modifications or new creations that can be protected by intellectual property rights. Therefore, it is worth determining who is to be the owner of the jointly created new intellectual property and establish the rules for sharing the related costs, such as who will bear the costs of filing for formal protection (e.g. as a trademark) and who will be indicated as the owner (one of the parties or a collective trademark). In the situation in question, the parties did not agree yet on issues such as the trade name for the final necklace, and will probably have to do so soon.

The joint-venture agreement should also specify who is liable if the intellectual property infringes the rights of third parties, and how the parties will share that liability. It is also worth determining the possible related costs.

Procedures for resolving disputes concerning intellectual property and the use of jointly created intellectual property should be regulated.

It is a good idea to establish confidentiality obligations for information disclosed in the joint venture and to define how confidential information will be protected (such as access restrictions, encryption, restrictions on publishing information without the consent of all parties to the joint venture, and publication approval procedures). It is also worth establishing procedures for responding to infringements of intellectual property rights by third parties.

Extremely important, but often overlooked, are provisions regarding exit from the joint venture, including establishing procedures for discontinuation of use by the withdrawing party of the intellectual property licensed from the other parties. It is worth considering competition clauses to limit the activities of the withdrawing party after leaving the joint venture.

3. Who owns the rights to the necklace designs created under the cooperation agreement with Golden Necklace?

The answer to this question depends on the course of the creative process that led to development of the product (necklace with detector add-on), as well as the wording of the contract. As a general rule, if several entities participated in development of a product, they should be jointly entitled to the rights to the product.

The case study here does not provide an answer to the question whether the detector (an accessory to the necklace, where the necklace could also be worn without the detector) affects the external appearance of the necklace and modifies its design. If so, it should be assumed that both entities jointly have rights to the design of the necklace with the detector. But the parties could stipulate differently in their agreement on who is entitled to these rights, as well as grant mutual licences to use the intellectual property created by each party, or transfer the rights of one party to other parties.

4. What should Medical Software pay special attention to as the licensee of the general-purpose AI model it relies on to develop its own AI system?

In addition to stating the mutual obligations of the parties typical of the licensor-licensee relationship (e.g. scope of use, territory, and duration of the licence), the agreement between Medical Software and Algorithmics should also address the obligations arising from treatment of Algorithmics as a provider of a general-purpose AI model, and Medical Software as a provider of a high-risk AI system.

In particular, Medical Software should ensure that Algorithmics provides and updates information and documentation regarding the licensed general-purpose AI model. In this respect, Algorithmics should provide documents and information enabling Medical Software to:

- Understand the capabilities and limitations of the licensed AI model, and
- Comply with the numerous obligations it will bear when it is deemed to be a provider of a high-risk AI system.

The documents to be provided by Algorithmics should contain at least the information specified in Annex XII to the AI Act, i.e.:

- A general description of the general-purpose AI model, including:
  - The tasks that the model is intended to perform and the type and nature of AI systems into which it can be integrated
  - The acceptable-use policies applicable
  - The date of release and methods of distribution
  - How the model interacts, or can be used to interact, with hardware or software that is not part of the model itself, where applicable
  - The versions of relevant software related to the use of the general-purpose AI model, where applicable
  - The architecture and number of parameters
  - The modality (e.g. text, image) and format of inputs and outputs
- A description of the elements of the model and of the process for its development, including:
  - The technical means (e.g. instructions for use, infrastructure, tools) required for the general-purpose AI model to be integrated into AI systems
  - Information on the data used for training, testing and validation, where applicable, including the type and provenance of data and curation methodologies.

This is particularly relevant, as the licence will be governed by Delaware law and Algorithmics is a US-based entity to which the AI Act applies only in connection with placement of a general-purpose AI model on the EU market.

The parties may also contractually regulate the use of data obtained from end users for further training of the model by Algorithmics.

5. Does the product's use of open-source software have any bearing on the rights held by the owner of the software?

Depending on what type of open-source software has been used, the use of open-source software can affect the issue of distribution of the software as a whole and the possibility of commercialising it. This is because some fragments of the source code are made available under a "copyleft" licence, which imposes on entities using open-source software the obligation to make the software they develop using the open source available to others on the same terms. Copyleft licences include such standards as GNU GPL, GNU LGPL, and GNU FDL.

Authors

Joanna Krakowiak
attorney-at-law, partner,
life sciences and healthcare

Krzysztof Wojdyło
adwokat, partner
new technologies

Marcin Rytel
adwokat,
life sciences and healthcare

Natalia Nieróbca
lawyer,
life sciences and healthcare

Karolina Romanowska
adwokat,
data protection

Łukasz Rutkowski
attorney-at-law,
data protection

Ewa Nagy
attorney-at-law,
intellectual property

Wardyński & Partners
Al. Ujazdowskie 10, 00-478 Warsaw
Tel.: +48 22 437 82 00, +48 22 537 82 00
Fax: +48 22 437 82 01, +48 22 537 82 01
E-mail warsaw@wardynski.com.pl