University of Gothenburg
School of Business, Economics and Law

Business and Innovation Law II, 30 hec

Department of Law

Legal compliance and commercial transactions of technology as legal resources in medtech

REPORT TO THE BOARD OF SIEMENS HEALTHCARE AB

ARTA EKMAN

UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

Table of Contents

Executive summary

The next-generation SOMATOM X.cite engages the MDR, the AI Act, the GDPR and NIS2 simultaneously, with the Cyber Resilience Act applying to supporting digital components not fully governed by the sector-specific cybersecurity requirements of the MDR. The strategic compliance risk is one of convergence: the same product decision typically triggers obligations under several instruments at once. Five priority workstreams follow.

1. **MDR / AI Act convergence**
   The regulatory regime requires an integrated rather than sequential compliance posture. Siemens should design a single combined technical-documentation file from project initiation, engage the notified body on a unified conformity-assessment pathway, and align intended-purpose drafting, software classification, AI risk management, human-oversight design and cybersecurity documentation through one governance workstream rather than through parallel functional silos.
2. **Clinical evidence, post-market surveillance and model drift**
   The regulatory regime requires continuing performance accountability for AI-enabled medical devices. Siemens should operate MDR post-market surveillance and AI Act post-market monitoring through a single process, define clinically meaningful performance indicators (dose distribution, image-quality consistency, scan-repeat rates, override frequency, cross-site performance, post-update accuracy), and pre-define the triggers for vigilance reporting, customer notification, rollback, updated instructions for use and renewed conformity assessment.
3. **Health-data governance**
   Lawful provenance of training, validation and improvement data is a precondition under the regulatory regime, and cannot be remediated retrospectively. Siemens should adopt a group-level framework that separates clinical, service, PMS, AI-training and telemetry data streams; require a dataset-provenance file for each training and validation dataset; standardise hospital data-access agreements distinguishing the permitted use of each stream; and integrate privacy-preserving techniques (federated learning, synthetic data, secure processing environments) into the AI development pipeline.
4. **Cybersecurity and hospital-network integration**
   The applicable regimes require an integrated security architecture rather than discrete product-level measures. Siemens should classify every external interface as open, restricted, Siemens-certified, proprietary or isolated, with documented legal and technical justification; embed cybersecurity into the product architecture, the remote-service infrastructure and the software-update channel; and align incident-response procedures with NIS2 reporting timelines and customer contractual commitments.

5. **Intellectual-asset control**
   The protection of know-how, software, datasets and model-related assets requires positive capture rather than passive reliance on default ownership. Siemens should establish a cross-divisional IAM register covering patents, software, datasets, model weights, workflow logic and trade-secret know-how, with metadata on creator, owner, IPRs, contractual encumbrances and trade-secret status; implement invention-disclosure and trade-secret-identification processes at R&D level; and operate background/foreground asset mapping for all collaborations.

Bargeddie Technologies Ltd. transaction

The patent does not enable BTL on its own; the commercial value is concentrated in unpatented know-how. The transaction should accordingly proceed only on the following terms:

(i) a fully executed NDA before any further substantive technical disclosure;
(ii) a field-of-use licence limited to non-destructive industrial testing, with medical, diagnostic, veterinary, human-imaging and security-screening uses expressly excluded;
(iii) staged territory beginning with the United States, with further expansion conditioned on demonstrated performance and an export-control assessment;
(iv) royalty-bearing financial terms supported by an upfront payment, milestone triggers and minimum annual payments;
(v) a non-exclusive, royalty-free, worldwide, sublicensable grant-back of improvements with notification and audit rights; and
(vi) compliance obligations – regulatory, trade-secret, export-control, anti-corruption – passed through to BTL's contract manufacturers and any permitted sublicensees.

Future role of the company lawyer

Legal work in technology-convergent industries is constitutive rather than advisory. Siemens should embed legal counsel in major product programmes through cross-functional product legal squads; centralise specialist competence in AI governance, regulatory strategy, IAM, cybersecurity and template contracting; retain local counsel for jurisdiction-specific matters such as healthcare-administrative law, public procurement, labour law and national implementation of EU obligations; establish a centralised product repository as the operational infrastructure for this model, covering active development projects, marketed products and discontinued products, and linking technical documentation, regulatory evidence, data-flow records, cybersecurity assessments, contracts and IAM records through role-based access control; and adopt the role description of the company lawyer as a governance architect – a designer of legal subjects, legal objects and legal relations through which technology is developed, commercialised and controlled.

1 Introduction

1.1 Mandate and role perspective

Siemens Healthcare AB stands at a regulatory inflection point. The next generation of the SOMATOM X.cite computed-tomography platform, including the AI-driven workflow assistant myExam Companion, will be the first product in the Siemens Healthineers portfolio to be developed, certified and commercialised under the full and simultaneous application of the Medical Device Regulation, the Artificial Intelligence Act, the General Data Protection Regulation, the NIS2 Directive and, in respect of supporting digital components, the Cyber Resilience Act. In parallel, the group has been approached on a non-core technology asset — United States Patent No. 9 842 720 and its associated X-ray-tube know-how — with a view to commercialisation by Bargeddie Technologies Ltd. in the non-destructive industrial testing market, a field distinct from the company's medical-imaging core. The Legal Division of Siemens Healthcare AB has accordingly assessed what this combined posture requires of the product, of the organisation and of the company's commercial counterparties, and reports its findings to the Board of Siemens Healthcare AB on the understanding that the Board will, in turn, bring those findings to the Board of Siemens Healthineers AG.

The analysis is organised around three questions. First, what is the legal-compliance architecture that the next-generation product must satisfy, and how must Siemens organise its product-development, conformity-assessment and post-market processes to satisfy it. Second, on what legal-object and legal-subject basis may Siemens out-license the patent and its associated know-how to Bargeddie Technologies Ltd., given that the unpatented know-how carries materially more commercial weight than the patent itself and that the counterparty is positioning itself to evolve from component supplier to end-product manufacturer. Third, what the cumulative picture from these two workstreams implies for the function, the competencies and the organisation of the company lawyer in a multinational MedTech group. The three workstreams were initially scoped in consultation with Christoffer Hermansson, Head of the Medical Device and AI Unit, who flagged them as the legal questions on which Board-level decisions are most directly dependent.

The perspective is that of the in-house lawyer who supports the business-development team in a multinational industrial company active on international markets. The function of the Legal Division is, on this account, twofold: to assess the legal-compliance posture of products and services, and to identify and structure the legal mechanisms through which the group's intellectual assets are commercialised. That dual function is the connecting theme across the three parts of this report.

1.2 Scope, assumptions and delimitations

The compliance analysis in Part I is limited to European Union law as the primary regulatory perimeter, on the assumption that the European Economic Area constitutes the principal placing-on-the-market jurisdiction for the SOMATOM X.cite. Union regulatory standards in the medical-device, artificial-intelligence and data-protection fields are, in general, more stringent than those of non-Union jurisdictions, with the consequence that compliance with the Union regime tends to satisfy the substantive requirements of most other markets in which the product will be sold.[1] Non-Union law is therefore addressed only where it imposes more demanding substantive requirements than the Union regime, or where it is otherwise strategically necessary – notably in the licensing analysis in Part II, where the territorial reach of United States patent No. 9 842 720 and the negotiating preferences of Bargeddie Technologies Ltd. require consideration of United States and, conditionally, Chinese market exposure.

The product is treated as an integrated medical-device ecosystem comprising the CT hardware, the myExam Companion software functionalities, remote-service connectivity to hospital information systems, and the underlying patient-data flows used for model training, validation and post-market surveillance. The technology that is the subject of the licence transaction in Part II is delimited to US patent No. 9 842 720 (X-ray tube unit) and its associated know-how concerning electric-discharge tubes, X-ray-tube technique and tube units; medical-field applications fall outside the licensed scope, as the patent shall be commercialised exclusively in the non-destructive testing market.

The report does not undertake a comparative analysis of national implementations of the EU instruments cited, nor does it address competition law beyond the question of vertical restraints in the licence transaction. Detailed clinical-evaluation strategy, conformity-assessment route selection with a specific notified body, and the financial modelling of royalty rates are likewise outside scope and are flagged where they ought to be developed in subsequent workstreams.

[1] See A Bradford, The Brussels Effect, 107 Northwestern University Law Review 1 (2012); A Bradford, The Brussels Effect: How the European Union Rules the World (OUP 2020). On the GDPR specifically, see ML Rustad and TH Koenig, Towards a Global Data Privacy Standard, 71 Florida Law Review 365 (2019); M Birnhack and G Mundlak, The Brussels Effect(s) and the Rise of a Privacy Profession, 15 International Data Privacy Law 138 (2025). On the AI Act, see C Siegmann and M Anderljung, The Brussels Effect and Artificial Intelligence (Centre for the Governance of AI Working Paper, 2022); for a more sceptical view, see A Engler, The EU AI Act Will Have Global Impact, But a Limited Brussels Effect (Brookings Institution, 2022). On the MDR's heightened stringency relative to predecessor and non-EU regimes, see C Hauskeller and others, Will the EU Medical Device Regulation Help to Improve the Safety and Performance of Medical AI Devices?, 4 Digital Health (2022).

1.3 Method and analytical framework

The report is methodologically grounded in doctrinal legal analysis, supplemented by the conceptual framework of intellectual-asset management developed across the Chalmers-track. The doctrinal layer identifies the applicable legal sources – Union legislation, harmonised standards, soft-law guidance from the Medical Device Coordination Group, the European Data Protection Board and the European Artificial Intelligence Office – and reasons from them to the concrete obligations of Siemens Healthcare AB and to the contractual mechanics of the BTL transaction. The asset-management layer characterises technology as a legal resource that can be captured, positioned, leveraged and organised through legal instruments.

Within the asset-management lens, the report makes analytical use of the distinction between legal subjects and legal objects. The licence transaction in Part II is organised around this distinction. The same conceptual lens carries over to Part III, where the role of the company lawyer is reconstructed as that of an architect of legal subjects, legal objects and legal relations in technology-driven business operations.

1.4 Disposition

The remainder of the report is organised in three parts and a concluding section. Part I (Section 2) analyses the compliance architecture for the next generation of the SOMATOM X.cite, beginning with the technical profile of the product and proceeding through legal frameworks, conformity-assessment standards, responsibility allocation, priority areas and organisational implications. Part II (Section 3) develops the BTL technology licence, treating in turn the transaction context, the legal-object characterisation of the licensed technology, the legal-subject structuring of the collaboration, the negotiation strategy, a clause-by-clause draft with commentary, and a synthesis. Part III (Section 4) reflects on the future role of the company lawyer on the basis of the findings in Parts I and II. Section 5 sets out the consolidated recommendations to the Board.

2 Part I – Legal Compliance Architecture for the Next Generation of SOMATOM X.cite

The Board has requested an assessment of the legal compliance architecture required for the next generation of SOMATOM X.cite, including myExam Companion. The analysis below proceeds from the product architecture rather than from the legal frameworks in the abstract. This is necessary because the legal consequences are generated by the convergence of CT hardware, AI-enabled software, hospital-network connectivity, remote-service infrastructure and data-driven improvement cycles.

The central conclusion is that Siemens should not treat the next-generation product as a scanner with added digital functions. It should be treated as an integrated AI-enabled medical-device ecosystem. This means that compliance must be designed as a lifecycle architecture: the same product decision may simultaneously affect MDR classification, AI Act high-risk status, GDPR role allocation, cybersecurity obligations, customer contracts, post-market monitoring and intellectual-asset control.

2.1 Product, technology and risk profile

The applicable legal regime cannot be identified before the regulated object has itself been characterised. SOMATOM X.cite is not legally relevant only because it is a CT scanner. It is legally relevant because it combines ionising-radiation hardware, AI-assisted clinical workflow, software-based image processing, hospital-network integration, remote-service capabilities and data feedback loops. The product is therefore regulated not as a single homogeneous object, but as a layered system in which different legal frameworks attach to different technical functions.

The Case 2A materials describe SOMATOM X.cite including myExam Companion as an industrial radiology-based product with capacity to interact with digital interfaces, perform CT scanning through computer processing, include AI-based image-processing and analytics functions, act as a software-based decision-support system, and participate in IoT/IoMT environments. The product and service components include the X-ray tube, Stellar detector, beam-shaping filters, collimators, control system, mobile control panel, AI workflow assistant, AI-Rad Companion, remote service and management, hospital-network data accessibility and other digital service integrations.

That factual starting point is decisive. The product's legal risk no longer arises only from the safety of the scanner as hardware. It arises from the interaction between the hardware, the software, the data, the operator, the hospital IT environment and Siemens' post-market control over the system.

2.1.1 SOMATOM X.cite as an integrated medical-device ecosystem

For legal purposes, the next-generation SOMATOM X.cite should be divided into six functional layers.

First, there is the CT hardware layer: the X-ray tube, detector array, gantry, patient table, filters, collimators and control system. This layer triggers the traditional medical-device and radiation-safety analysis. The device emits ionising radiation for diagnostic purposes and must therefore satisfy the safety, performance, quality-management, clinical-evaluation and post-market requirements of the MDR.

Secondly, there is the workflow-assistance layer, principally myExam Companion. This layer supports scan parameterisation, patient positioning, protocol selection, operator guidance and consistency across clinical settings. Its legal significance depends on its intended purpose. If it is framed as workflow assistance, the legal burden is substantial but remains connected to operator-guided use. If it is framed as diagnostic decision support, automated triage or clinically determinative recommendation, the classification and evidence burden increase.

Thirdly, there is the image-processing and reconstruction layer. Machine-learning-supported image enhancement, segmentation, reconstruction or recognition functionality can affect image quality, diagnostic reliability, dose optimisation and repeat-scan rates. It therefore belongs both to MDR safety/performance analysis and to AI Act high-risk analysis.

Fourthly, there is the data layer. Training datasets, validation cohorts, post-market data streams, performance logs, user-interaction data and clinical feedback are not merely technical inputs. They become legal evidence under the AI Act, regulated personal data under the GDPR, potential database assets, and commercially valuable know-how.

Fifthly, there is the connectivity layer. Hospital information systems, PACS, EHR infrastructure, DICOM exchange, remote-service access and software-update channels create a cybersecurity and data-governance perimeter extending beyond the physical scanner. The scanner becomes a node in the hospital’s digital infrastructure.

Sixthly, there is the service and lifecycle layer. Remote monitoring, software updates, predictive maintenance, post-market surveillance, incident reporting and continuous AI performance monitoring mean that the product continues to evolve after market placement. This shifts the compliance focus from one-time market entry to continuous legal accountability.

The consequence is that Siemens must not build a compliance file around the scanner alone. It must build a compliance file around the interaction between scanner, software, data, hospital environment and post-market control.

2.1.2 Technology-asset categories

The Case 2A technology tree supports this layered analysis. It classifies the product's intellectual and technical resources into hardware-related solutions, IT-related solutions, network and communication-related solutions, software-based instructions, processed data and databases. The Case 2A hand-in connects these categories to CPC areas such as A61B for medical/radiation diagnosis, G06T for image data processing, G06N for neural-network and computational-model systems, G06F/G06K/G06V for digital data processing and recognition, G16H for healthcare informatics, G21K for ionising-radiation techniques, and H01J/H05G for X-ray tubes and X-ray technique.

This matters because the legal control mechanism differs between asset categories. Hardware-related solutions are often controlled through patents, design rights, manufacturing know-how, quality systems and MDR technical documentation. Software-based instructions are controlled through copyright, trade secrets, possible computer-implemented invention patents, software lifecycle processes and cybersecurity measures. Data and databases are controlled through GDPR-compliant access rights, database rights where applicable, trade secrets, contracts and technical access controls. Network and communication solutions are controlled through cybersecurity architecture, interoperability choices, customer contracts and supplier obligations.

For the Board, the key point is that the product's value proposition is no longer located in one asset class. Competitive advantage lies in the orchestration of hardware, software, data, clinical workflow, user interface and service capability. The legal function must therefore maintain an asset map that connects each technology asset to its legal status, owner, creator, contractual encumbrances, compliance obligations and commercial use case. This follows the IAM logic in the Case 2A materials, where intellectual assets are to be identified, assessed and tagged with metadata such as value, control, creator, owner, IPRs, technology area and relevant contracts.

2.1.3 Core legal risk profile

The next-generation product creates a cumulative rather than discrete legal risk profile. The same technical decision can trigger several legal consequences.

For example a decision to expand myExam Companion from workflow support to diagnostic decision support may affect MDR classification, AI Act high-risk obligations, clinical evidence, human oversight, marketing claims and product-liability exposure. A decision to use real-world hospital data for model improvement may affect GDPR role allocation, Article 9 lawful processing, AI Act Article 10 data quality, hospital contracts, international-transfer arrangements and trade-secret strategy. A decision to enable remote software updates may affect cybersecurity

obligations, substantial-modification analysis, customer service-level commitments, incident reporting and post-market surveillance.

The legal question is therefore not only “which laws apply?” The more important question is “which technical and organisational choices determine the legal position of the product?” For the Board, that means compliance must be treated as part of the product-development strategy rather than as a separate legal review after design decisions have already been made.

2.2 Applicable legal frameworks and jurisdictions

2.2.1 EU market as the primary compliance perimeter

The European Union is treated as the primary compliance perimeter. The central regimes are the MDR, the AI Act, the GDPR and NIS2. Supporting frameworks include the Data Act, the European Health Data Space Regulation to the extent relevant at the time of implementation, product-liability law, trade-secret law, intellectual-property law, public-procurement law, healthcare-administrative law and contract law.

This does not mean that non-EU regimes are necessarily less demanding in every aspect. However, a full comparative analysis falls outside the scope of this report. The EU regime is used as the operative baseline because it is strategically important for market access and because its regulatory structure captures the main risks of AI-enabled medical-device development.

The assignment instructions specifically identify product safety regulation, AI regulation, GDPR, cybersecurity law, intellectual property law, trade-secret law, contract law, labour law, property law and legislation relating to healthcare and authority administration as relevant to varying extents. The sections below focus on the frameworks that generate the most direct legal-accountability issues for the next-generation product.

2.2.2 Product-safety and medical-device law

Regulation (EU) 2017/745 on medical devices (MDR) is the foundational legal framework. The physical SOMATOM X.cite falls within the MDR because it is intended for diagnostic medical use. For the purposes of this report, Siemens Healthcare AB is assumed either to act as the manufacturer or to coordinate manufacturer obligations within the Siemens Healthineers group. The precise legal-entity allocation must be confirmed internally before market placement.

For the current SOMATOM X.cite, the Case 2A hand-in characterises the device as an active device intended to emit ionising radiation for diagnostic purposes under Annex VIII Rule 10, resulting in Class IIb classification. For the next-generation product, this hardware classification remains important, but the more delicate question concerns the software and AI functions. MDR

Rule 11 may apply to software intended to provide information used for diagnostic or therapeutic decisions. The legal risk is therefore highly sensitive to the intended purpose of myExam Companion and any additional AI functions.

The decisive MDR question is not whether the CT scanner is a medical device. That is straightforward. The decisive question is how Siemens defines the intended purpose of the software layer. If myExam Companion is positioned as an operator-support tool that improves consistency, guides scan preparation and assists workflow, the regulatory burden remains substantial but more manageable within the device's overall conformity assessment. If the next-generation product is positioned as diagnostic decision support, autonomous image interpretation, automated triage or recommendation of therapeutic pathways, the software classification, clinical evidence burden and liability exposure increase significantly.

Legal should therefore review the intended-purpose statement, technical design, instructions for use, marketing material, sales claims and user-interface language together. Intended purpose is not merely a communications issue. It is a regulatory classification issue. A claim that the system "assists protocol selection" creates a different legal profile from a claim that the system "detects disease," "recommends diagnosis" or "determines clinical urgency."

Conformity assessment must then be organised around the product as actually designed and marketed. Class IIa and above devices require notified-body involvement. The General Safety and Performance Requirements in Annex I govern safety, performance, risk management, usability, information supplied with the device and software lifecycle requirements. For software and connected functionality, Annex I section 17 is particularly important because it requires state-of-the-art development, verification, validation and cybersecurity measures.

Clinical evaluation under MDR Article 61 and Annex XIV must be planned and updated in light of the product's intended purpose. For AI-enabled software, this means that clinical evidence cannot be limited to the physical scanner's baseline performance. Siemens must be able to show that the software functions perform safely and effectively in the intended clinical workflow, with the intended users, patient groups and operating environments.

Post-market surveillance under MDR Articles 83–86 and vigilance obligations under Articles 87–92 are equally central. For the next-generation product, PMS must be designed to detect not only hardware malfunction but also software-related performance issues, usability problems, cybersecurity vulnerabilities, automation bias and unintended consequences of updates. MDR compliance therefore becomes a lifecycle function, not only a pre-market certification exercise.

2.2.3 AI governance

Regulation (EU) 2024/1689, the AI Act, creates the second central compliance layer. An AI system is high-risk under Article 6 where it is a product, or safety component of a product, covered by Union harmonisation legislation listed in Annex I and the product is subject to third-party conformity assessment. Medical devices under the MDR fall within this structure.

For the purposes of this report, myExam Companion and any next-generation AI functions should therefore be treated as likely high-risk where they are part of the MDR conformity assessment or function as safety-relevant components of the medical device. The final assessment depends on the exact intended purpose, technical integration and conformity-assessment route.

The high-risk regime imposes obligations concerning risk management, data governance, technical documentation, record keeping, transparency, instructions for use, human oversight, accuracy, robustness, cybersecurity and post-market monitoring. The operational consequence is that Siemens must build an AI evidence file, not merely an engineering file. That evidence file should connect the AI system's intended purpose, dataset provenance, dataset representativeness, bias assessment, validation methodology, human oversight design, logging, cybersecurity measures, model-performance monitoring and post-market update procedures.

The phased application of the AI Act must also be tracked against the product-development and market-placement timeline. The obligations applicable to high-risk AI systems do not all apply from a single date, and the legal relevance of several provisions depends on when the next-generation product is placed on the market or substantially modified. The combined MDR/AI Act conformity-assessment pathway should therefore be planned against the calendar of AI Act application rather than against the date of project initiation, and the technical documentation should be capable of demonstrating compliance with the obligations applicable on each successive trigger date.

For Siemens, Article 10 data governance is particularly important. The legal issue is not simply whether the model works in engineering tests. Siemens must be able to demonstrate why the training, validation and testing data are appropriate for the intended clinical context. In a CT environment, this includes variation in patient anatomy, body size, age, clinical indication, scanner configuration, operator experience, image-quality requirements and hospital workflow. If the model performs well in one setting but degrades in another, the issue is not only technical. It becomes a regulatory-evidence problem.

Human oversight under Article 14 AI Act must be operationalised as a substantive control rather than as a formal disclaimer. The instructions for use, the user-interface design and the hospital training materials must make clear when myExam Companion supports the operator, when

professional judgment is required, and which outputs should not be treated as autonomous clinical determinations. This is the operative link between AI Act human-oversight obligations, MDR usability engineering and the allocation of clinical responsibility between Siemens as provider and the hospital as deployer. Where interface design or marketing language makes the AI output appear more authoritative than its validated performance supports, automation bias becomes both a patient-safety risk and a regulatory-evidence problem.

The AI Act therefore changes the evidentiary structure of the product. MDR evidence asks whether the device is safe and performs as intended. AI Act evidence asks whether the AI system is governed through appropriate data, documentation, transparency, human oversight, robustness and monitoring. These questions overlap, but they are not identical. Siemens should avoid preparing a traditional MDR technical file first and adding AI Act material afterwards. The combined evidentiary architecture should be designed from the beginning.

2.2.4 Data protection and health-data governance

Regulation (EU) 2016/679, the GDPR, applies wherever personal data is processed in the development, deployment, remote service, post-market monitoring or improvement of the product. Because CT images and associated clinical information relate to health, the relevant data will often be special-category data under Article 9 GDPR. Processing therefore requires both a lawful basis under Article 6 and an applicable Article 9 condition.

The data-governance problem should not be treated as one generic “GDPR issue.” The next-generation product creates several legally distinct data streams.

First, patient-care data is generated when the hospital uses the scanner for diagnosis. The hospital will ordinarily act as controller for clinical care, while Siemens may have no role, a processor role, or a separate controller role depending on the service arrangement.

Secondly, remote-service and maintenance data may be processed by Siemens to monitor uptime, detect faults, maintain system performance and deliver software updates. Depending on whether the data includes personal data or can be linked to patient examinations, Siemens may be processor, independent controller or joint controller.

Thirdly, post-market surveillance data is processed to satisfy MDR obligations. This may support an argument that certain processing is necessary for regulatory compliance, but the GDPR analysis must still identify the appropriate legal basis, Article 9 condition, data minimisation and retention rules.

Fourthly, AI training and validation data may be used to improve myExam Companion or other AI functions. This is usually the most legally sensitive stream. Siemens may be acting as

controller or joint controller, and the lawful provenance of historical datasets must be documented. Explicit consent, scientific research grounds or public-health grounds may be available in specific circumstances, but none should be assumed without analysis.

Fifthly, commercial telemetry and product analytics may be useful for business development, performance benchmarking and service optimisation. However, such data cannot automatically be repurposed for AI model development or commercial analytics if it was collected for a narrower service or clinical purpose.

The Board should therefore require data-flow separation. Each data stream should have its own purpose, role allocation, lawful basis, Article 9 condition, retention period, security level, access control, contractual treatment and documentation output. In practice, this means that every hospital deployment should be accompanied by a data-processing architecture that distinguishes clinical use, service use, PMS use, AI-training use and commercial telemetry use.

Where high-risk processing occurs, a data-protection impact assessment under Article 35 GDPR will generally be required. For hospital collaborations, Siemens must also document controller/processor or joint-controller allocation, restrictions on secondary use, anonymisation or pseudonymisation strategy, international-transfer mechanisms and data-subject-rights procedures.

The European Health Data Space may become relevant as a framework for primary and secondary use of electronic health data, but it should not be treated as a shortcut around GDPR compliance. It should be treated as an additional framework that may facilitate structured data access where implemented and applicable.

2.2.5 Cybersecurity and digital resilience

Cybersecurity obligations apply at both product level and organisational level. At product level, MDR Annex I section 17 requires software and devices incorporating software to be developed and manufactured according to the state of the art, taking into account lifecycle, risk management, verification, validation and cybersecurity. MDCG guidance, particularly MDCG 2019-16 on cybersecurity for medical devices, should be used to operationalise these obligations.

At organisational level, NIS2 requires relevant entities to implement cybersecurity risk-management measures and incident-reporting procedures. The Directive includes manufacturing of medical devices and in vitro diagnostic medical devices within Annex II, making NIS2 relevance for Siemens Healthcare AB a concrete issue to be assessed rather than a remote possibility. The precise Swedish implementing obligations must be confirmed against the national NIS2 instrument applicable at the time of market placement. For present purposes, the Board should assume that Siemens Healthcare AB will be required to maintain documented

cybersecurity risk-management measures, incident-reporting procedures aligned with the timelines in Article 23 NIS2, and management-body involvement in cybersecurity governance as required under Article 20 NIS2.

The Cyber Resilience Act must also be assessed. Regulation (EU) 2024/2847 establishes horizontal cybersecurity requirements for products with digital elements. However, the CRA contains exclusions and interaction rules for products already covered by sector-specific Union legislation, including medical devices, so the precise application to SOMATOM X.cite and to accessories or peripheral digital products must be assessed component by component.

For the Board, the practical point is that cybersecurity is not merely an IT issue. A cybersecurity failure may simultaneously become a patient-safety issue, MDR non-conformity, GDPR data breach, AI-integrity failure, customer-contract breach and reputational crisis. Cybersecurity must therefore be embedded in product architecture, hospital integration, supplier management, software update governance and incident response.

2.2.6 Supporting legal areas

In addition to the four principal layers above, several supporting legal areas are relevant.

Intellectual property and trade-secret law govern patents, software, documentation, model weights, training methods, workflow logic, datasets and tacit know-how. The Case 2A materials stress that intellectual assets include not only registered IPRs but also valuable know-how, data, databases, observations, theoretical frameworks, solutions, instructions and software, some of which may exist only in employees' heads or may not yet be explicitly managed as trade secrets or copyrightable works.

Contract law governs customer agreements, hospital data-access agreements, remote-service terms, software-update terms, supplier agreements, processor agreements, R&D collaborations, public procurement participation and intra-group IP arrangements.

Product-liability law is relevant because the product may cause harm through hardware malfunction, radiation exposure, software error, AI output, cybersecurity compromise or inadequate instructions for use. The new EU product-liability framework strengthens the need for documentation and responsibility allocation for digital and AI-enabled products.

Public procurement and healthcare-administrative law are relevant because public healthcare providers are often customers. Contractual and commercial models must therefore be compatible with procurement transparency, public-sector purchasing procedures, clinical responsibility and restrictions on improper inducements.

Competition law and data-access law may become relevant if Siemens uses a closed hardware/software ecosystem to restrict interoperability or third-party access. A Siemens-controlled interface model may be defensible for cybersecurity and safety reasons, but must be designed and documented as risk-based rather than purely exclusionary.

Labour law and occupational-health considerations arise indirectly because AI-guided workflow tools may change the role of radiographers and clinical staff. This affects usability, training, human oversight, instructions for use and hospital adoption.

2.2.7 Compliance map

The following table translates the product architecture into legal consequences. It is not intended to be exhaustive. Its function is to identify the legal decision points that must be managed by the product legal team.

Product layer / feature	Principal legal risk	Documentation output	Contractual instrument	Board-level consequence
CT hardware emitting ionising radiation	MDR classification, radiation safety, patient/operator injury	MDR technical file, GSPR matrix, clinical evaluation, risk-management file	Customer terms, service terms, supplier quality clauses	Confirm manufacturer responsibility and notified-body strategy
myExam Companion workflow support	MDR software qualification, AI Act high-risk status, human oversight	Intended-purpose memo, software classification memo, AI risk file, human-oversight design evidence	AI-use terms, instructions for use, hospital responsibility clauses	Approve intended-purpose strategy before product claims are finalised
Image reconstruction / AI image processing	Insufficient clinical evidence, model drift, automation bias	Clinical validation plan, dataset file, model-performance report, PMS indicators	Update terms, PMS cooperation clauses, data-access terms	Approve combined MDR/AI Act evidence architecture
Training and validation data	Unlawful Article 9 processing, biased or non-representative data, weak provenance	DPIA, dataset provenance file, lawful-basis assessment, representativeness/bias assessment	Hospital data-access agreement, joint-controller or processor terms	Approve data-governance model before data is collected or reused
Remote service and software updates	Cybersecurity compromise, substantial modification, unsafe update	Update impact assessment, cybersecurity file, vulnerability process, incident log	Remote-service agreement, SLA, update clause, security annex	Approve software-update governance and escalation process
Hospital-network integration	Undefined security boundary, data leakage, NIS2 customer expectations	Network security model, interface specification, access-control documentation	Security agreement, processor terms, customer	Approve risk-tiered connectivity model

Product layer / feature	Principal legal risk	Documentation output	Contractual instrument	Board-level consequence
			configuration obligations	
Post-market data streams	Secondary-use risk, PMS gaps, AI Act monitoring gaps	PMS plan, AI post-market monitoring plan, performance dashboard, incident file	PMS cooperation clause, data-use clause, reporting obligations	Approve continuous monitoring capability
Cross-divisional R&D assets	Loss of trade secrets, unclear ownership, weak patent capture, siloing	IAM register, invention-disclosure file, background/foreground asset map	R&D collaboration terms, intra-group IP licence, confidentiality terms	Approve group-level IAM process
Supplier software / components	Undefined responsibility, cybersecurity gap, quality failure	Supplier qualification file, software bill of materials where relevant, quality agreement	Supplier quality agreement, cybersecurity clause, audit rights	Approve supplier compliance playbook
Closed/proprietary interface model	Interoperability, procurement, Data Act and competition-law tensions	Interface-risk assessment, legal justification memo	API terms, integration agreement, access restrictions	Decide whether control strategy is safety-driven, commercial or both

The map shows that the legal department must not merely advise on legislation. It must structure documentation, contracts and internal decisions in parallel with product development.

2.3 Standards and guidance as conformity tools

2.3.1 Legal function of harmonised standards

Harmonised standards are not themselves the source of legal obligations. Their function is evidentiary and operational. Under the MDR, compliance with relevant harmonised standards may provide a presumption of conformity with the legal requirements to which those standards relate. The legal obligation remains in the Regulation; the standard helps Siemens demonstrate how the obligation has been satisfied.

This distinction matters for the next-generation SOMATOM X.cite. If Siemens follows a standard, that may strengthen the conformity case. But a standard cannot determine the intended purpose of myExam Companion, the MDR classification of a software function, whether the AI Act applies as high-risk, whether training data is lawfully processed under GDPR, or whether a software update is a substantial modification. Those remain legal assessments.

2.3.2 Medical-device and software standards

The core medical-device standards should include ISO 13485 for quality management systems, ISO 14971 for medical-device risk management, IEC 62304 for medical-device software lifecycle processes, IEC 62366-1 for usability engineering, IEC 60601-1 for basic safety and essential performance of medical electrical equipment, IEC 60601-2-44 for CT equipment and IEC 81001-5-1 for cybersecurity activities in health software and health IT systems.

For Siemens, these standards should not be treated as a compliance checklist at the end of development. They should be translated into product-development gates. For example, risk-management outputs should inform intended-purpose design, software validation, AI human oversight, cybersecurity architecture, clinical evaluation and instructions for use. Usability engineering is particularly important because a workflow assistant can create operator reliance. If the interface makes the AI output appear more authoritative than intended, the legal risk increases even if the underlying model is technically sound.

2.3.3 AI and data-governance standards

For AI governance, ISO/IEC 42001 provides a framework for an AI management system, ISO/IEC 23894 addresses AI risk management, and ISO/IEC 5259 addresses data quality for analytics and machine learning. ISO/IEC 27001 and ISO/IEC 27701 remain important for information security and privacy governance. Future harmonised standards under the AI Act should be monitored and incorporated into Siemens' QMS as they become available.

The practical objective should be to create repeatable internal processes. For each AI function, Siemens should be able to show: intended purpose, model version, training data sources, validation dataset, representativeness assessment, known limitations, human oversight design, logging, cybersecurity controls, performance monitoring and update triggers.

2.3.4 Soft-law guidance

Guidance from the Medical Device Coordination Group, the European Data Protection Board and the European AI Office should be treated as practical interpretive material. MDCG guidance on software qualification and classification, cybersecurity for medical devices and clinical evaluation of medical-device software is particularly relevant. EDPB guidance should inform controller/processor allocation, anonymisation, DPIAs, health-data processing and international transfers. EU AI Office guidance and joint guidance on the interaction between the MDR and AI Act should be monitored as implementation develops. The European Commission has already issued guidance addressing the interplay between medical-device AI and the AI Act.

The legal effect of such guidance is not the same as binding legislation. However, deviation from it is operationally costly. Notified bodies, regulators and customers will often use guidance as evidence of expected practice. Siemens should therefore institutionalise relevant guidance into standard operating procedures and document any reasoned deviations.

2.3.5 Limits of standards

Standards and guidance cannot answer the most important legal qualification questions. They do not determine whether a specific software function is medical-device software, whether myExam Companion is high-risk AI, whether Siemens is controller or processor for a specific data flow, whether a hospital dataset is sufficiently anonymised, whether a software update changes the intended purpose, whether a closed interface model raises competition-law concerns, or whether a specific contractual allocation of responsibility is enforceable.

The legal function must therefore be able to read standards critically. It should not delegate legal qualification to engineering, quality management or regulatory affairs. The better model is joint assessment: regulatory affairs and engineering define the technical facts; legal determines the legal consequences; the product team implements the decision through documentation, design and contracts.

2.4 Responsibility architecture: legal roles, functions and measures

2.4.1 Legal roles

The MDR creates economic-operator roles, including manufacturer, authorised representative, importer, distributor and person responsible for regulatory compliance. For the purposes of this report, Siemens Healthcare AB is assumed to be the entity responsible for coordinating the relevant manufacturer obligations within the Siemens group, but the final legal-entity allocation must be verified internally. The PRRC function under MDR Article 15 must be empowered with access to technical documentation, conformity assessment, post-market surveillance and vigilance data.

The AI Act creates parallel AI value-chain roles, including provider, deployer, importer and distributor. Where Siemens places myExam Companion or another AI-enabled software function on the market under its name or trademark, Siemens is likely to be the provider. Hospitals using the system will ordinarily be deployers. If a hospital or third party substantially modifies the AI system or changes its intended purpose, responsibility may shift or be shared, but Siemens should not rely on this possibility as a default risk shield. Provider/deployer boundaries should be documented in customer contracts, instructions for use and internal legal memoranda.

The GDPR creates controller, processor and joint-controller roles. These roles are not determined by contractual labels alone. They depend on who determines the purposes and means of processing. Siemens may be processor for remote service, independent controller for product improvement, joint controller for certain research collaborations, and no personal-data actor for fully anonymised datasets. The legal department must therefore map roles per data stream, not per customer relationship.

NIS2 adds organisational cybersecurity responsibility, including risk-management and incident-reporting obligations where Siemens falls within scope. Management-body involvement is important because cybersecurity risk is now a governance issue, not merely a technical-support matter.

2.4.2 Internal functions

The legal roles must be translated into internal functions. The required functions include regulatory affairs, quality management, clinical evaluation, PMS and vigilance, AI governance, data protection, cybersecurity, IP/IAM, procurement, contracting, R&D legal support, product marketing review and customer contracting.

The decisive factor is not whether Siemens has each function somewhere in the group. It is whether those functions are integrated around the product. A traditional division between regulatory counsel, privacy counsel, IP counsel and commercial counsel is insufficient where the same design decision affects MDR classification, AI Act documentation, GDPR data processing, cybersecurity architecture and customer obligations.

For the next-generation product, Siemens should create a cross-functional product legal workstream with defined responsibility for: intended-purpose review; MDR/AI Act evidence architecture; data-flow mapping; DPIA coordination; cybersecurity contracting; software-update governance; clinical-evidence legal review; supplier contract alignment; and IAM capture.

2.4.3 Required legal measures

The required legal measures should be organised as deliverables.

First, Siemens should prepare an intended-purpose and classification memorandum covering the physical device, software modules and AI functions.

Secondly, Siemens should prepare a combined MDR/AI Act evidence architecture that links the MDR technical documentation, AI Act technical documentation, risk-management file, clinical evaluation, AI validation, cybersecurity documentation and post-market monitoring.

Thirdly, Siemens should prepare a data-governance file for each data stream: clinical use, remote service, PMS, AI training/validation and product telemetry.

Fourthly, Siemens should prepare standard hospital contracting modules covering data processing, remote service, cybersecurity, software updates, PMS cooperation, AI-output use, human oversight and allocation of clinical responsibility.

Fifthly, Siemens should prepare supplier compliance clauses covering cybersecurity, quality, audit rights, software components, regulatory cooperation, data protection, confidentiality and IP ownership.

Sixthly, Siemens should prepare an IAM register linking technology assets to owners, creators, IPRs, trade-secret status, contractual restrictions, technical area and compliance relevance.

Lastly, Siemens should prepare a software-update governance process identifying when updates require regulatory review, customer notice, validation, cybersecurity assessment, AI performance testing or renewed conformity assessment.

2.4.4 Accountability across the product lifecycle

A static enumeration of legal roles misrepresents the operative legal regime. The MDR, AI Act and GDPR all operate across the product lifecycle.

At the design stage, Siemens must determine intended purpose, classification, AI-function boundaries, data sources, cybersecurity architecture, human oversight and asset ownership. The most important legal decisions are often made here, because later documentation must justify design choices that are already embedded in the product.

At the validation stage, Siemens must generate clinical and technical evidence showing that the product performs safely and effectively in the intended environment. For AI functions, validation must address dataset suitability, representativeness, bias, robustness, human oversight and failure modes.

At the market-placement stage, the conformity assessment, technical documentation, CE marking, instructions for use, customer contracts and commercial claims crystallise Siemens' legal position.

At the post-market stage, Siemens must monitor complaints, incidents, cybersecurity vulnerabilities, model performance, software updates, customer feedback, clinical performance and potential concept drift. For AI-enabled functions, post-market monitoring cannot be limited to ordinary complaint handling. It must be capable of detecting performance degradation and changed risk profiles.

At the update stage, Siemens must assess whether software or AI model changes affect safety, performance, intended purpose, cybersecurity, data processing, customer obligations or conformity assessment. A software update that improves image quality but affects dose, operator reliance or model explainability is not merely an engineering release. It is a legal event.

2.5 Priority compliance areas for next-generation development

2.5.1 Prioritisation method

The priority areas below are assessed according to four criteria: likelihood of non-conformity, severity of legal and patient-safety consequences, strategic importance for the product roadmap, and organisational readiness. The relevant question is not which legal frameworks are theoretically applicable. It is which compliance areas are most likely to determine whether Siemens can develop, produce, sell and continuously improve the next-generation product without unacceptable legal, financial or reputational exposure.

2.5.2 Priority 1: MDR/AI Act convergence

The convergence of MDR conformity assessment and AI Act high-risk obligations is the central compliance issue. The Case 2A hand-in already identifies that the next-generation SOMATOM X.cite and myExam Companion represent a convergence between advanced medical hardware and AI, requiring Siemens to move beyond reactive MDR compliance and address the AI Act, GDPR, Data Act and NIS2 as intersecting frameworks.

The Board should treat MDR/AI Act convergence as an evidentiary architecture problem. The AI Act contemplates integration with sectoral conformity assessment, but practical implementation remains complex. MDR evidence asks whether the device is safe and performs as intended. AI Act evidence asks whether the AI system is governed through appropriate data, documentation, transparency, human oversight, robustness, cybersecurity and monitoring. For myExam Companion, these requirements overlap but do not fully merge.

Siemens should therefore avoid building a conventional MDR technical file first and then adding an AI Act annex later. The combined file should be designed from the beginning. It should include: software module boundaries; intended-purpose analysis; AI high-risk assessment; dataset provenance; dataset representativeness; clinical validation; AI risk management; logging; human oversight; cybersecurity; post-market monitoring; software-update governance; and customer-use instructions.

The Board should approve an integrated MDR/AI Act compliance workstream with authority to engage the notified body early and define the combined audit pathway. This is not merely an

efficiency measure. It reduces the risk of contradictory documentation, delayed certification, weak post-market monitoring and unclear internal accountability.

2.5.3 Priority 2: Clinical evidence, post-market surveillance and model drift

The next-generation product depends on continuously improving AI-enabled functions. That creates a clinical-evidence challenge. Traditional clinical evaluation is not sufficient if the product's performance may evolve through software updates, changing datasets, new use environments and post-market learning.

In the SOMATOM context, model drift is not only a statistical issue. It may affect radiation dose, image quality, scan repeat rates, operator reliance, diagnostic reliability, workflow consistency and patient safety. A model that performs acceptably in validation may behave differently across hospitals with different patient populations, scanner configurations, protocols, operator experience and IT environments.

Siemens should therefore define post-market performance indicators that are clinically meaningful. These may include dose distribution, image-quality consistency, scan-repeat frequency, frequency of manual override, operator feedback, incident reports, performance across patient groups, performance across hospital sites, and changes in model accuracy following software updates.

These indicators should feed both MDR PMS and AI Act post-market monitoring. The Case 2A hand-in similarly identifies that post-market surveillance must expand beyond MDR requirements to include continuous monitoring of AI performance and concept drift to ensure ongoing accuracy and robustness.

The Board should require an AI post-market monitoring programme that is not separated from the PMS system. A single governance process should identify when performance issues trigger MDR vigilance, AI Act reporting, customer notification, software rollback, updated instructions for use or renewed conformity assessment.

2.5.4 Priority 3: Health-data governance for training, validation and improvement

The lawful provenance of training data is one of the most difficult areas to remediate retrospectively. If Siemens trains, validates or improves AI functions using data that was not lawfully obtained or cannot be adequately documented, the problem may affect both GDPR compliance and AI Act conformity.

The next-generation product should therefore be developed with a data-governance architecture before data is collected or reused. The legal function should require a dataset-provenance file for

each training and validation dataset. That file should identify: data source; controller/processor allocation; lawful basis; Article 9 condition; consent or research framework where relevant; anonymisation or pseudonymisation measures; representativeness; bias assessment; retention period; transfer mechanism; and contractual restrictions.

For hospital collaborations, Siemens should use data-access agreements that distinguish service use, PMS use, AI-training use and commercial analytics. A general service agreement should not be treated as sufficient legal basis for broad AI development. If Siemens wants to use post-market data to improve myExam Companion, that purpose must be contractually, technically and legally separated from ordinary maintenance.

Privacy-preserving techniques should be assessed as strategic tools. Federated learning, synthetic data, differential privacy and secure processing environments may reduce legal risk and improve customer acceptance. However, they do not eliminate GDPR analysis. Pseudonymised data remains personal data, and anonymisation must be robust in light of medical imaging re-identification risks.

The Board should approve a group-level health-data-governance framework for AI-enabled medical devices. Without such a framework, each hospital collaboration risks becoming a bespoke legal negotiation, slowing development and increasing inconsistency.

2.5.5 Priority 4: Cybersecurity and hospital-network integration

The SOMATOM X.cite is no longer a standalone scanner. Its cybersecurity perimeter extends to the hospital network, PACS/EHR interfaces, remote-service infrastructure, software-update channels, supplier components and any interface through which operational commands or data are exchanged. Cybersecurity is therefore part of the product's regulatory safety case.

The compliance regime under MDR Annex I section 17 must be integrated with NIS2 risk-management expectations and with the contractual security requirements imposed by hospital customers. The Case 2A hand-in identifies that digitised healthcare systems make cybersecurity paramount and that Siemens must embed cybersecurity into the product architecture through a security-by-design approach.

The legal question is not simply whether the product should be connected or disconnected. The product's commercial value depends on integration with hospital systems, remote service, software updates and data feedback. At the same time, each additional interface expands the attack surface and may create new responsibility boundaries.

Siemens should therefore adopt a risk-tiered connectivity model.

Low-risk data exchanges may be handled through standardised secure interfaces. Safety-critical communications should be restricted to certified and monitored channels. Remote-service access should require strong authentication, logging, access control, customer authorisation and incident-response commitments. Software-update channels should be validated, documented and subject to legal review where they may affect safety, AI performance or intended purpose. Full or partial isolation should be reserved for functions where the cybersecurity risk outweighs the operational value of connectivity.

A more closed Siemens-controlled ecosystem may be strategically attractive. Restricting integrations to approved Siemens-controlled interfaces, using proprietary encrypted communication channels and limiting external access may reduce attack surfaces and strengthen Siemens' ability to control cybersecurity risk. It may also support a hardware-as-lock strategy, where Siemens' hardware, software and service layers become commercially interdependent.

However, this strategy must be handled carefully. A fully proprietary or air-gapped model may conflict with interoperability expectations, hospital procurement requirements, data-access rights and competition-law concerns. It may also reduce the product's value if hospitals need integration with existing PACS, EHR, scheduling, reporting and AI systems.

The legal recommendation is therefore not to close the system by default. The recommendation is to classify interfaces by risk and business function. Each interface should be designated as open, restricted, Siemens-certified, proprietary or isolated, with a documented legal and technical justification. This makes cybersecurity architecture a board-level product strategy question, not merely a technical configuration issue.

2.5.6 Priority 5: IP/trade-secret control in cross-divisional R&D

The next-generation product depends on assets that are difficult to capture through ordinary patent-management processes. The technology tree shows that the product is not only an A61B medical-device hardware project. It also involves G06T image processing, G06N neural-network systems, G06F/G06K/G06V digital data and recognition technologies, G16H healthcare informatics, G21K ionising-radiation techniques and H01J/H05G X-ray technology.

This means that many strategic assets will exist as software, datasets, model weights, workflow logic, user-interface design, validation methods, clinical protocols, cybersecurity architecture and tacit employee know-how. These are not always neatly registered as patents. They may be spread across Siemens Healthcare AB, Siemens Healthineers, Siemens AG divisions, Varian-related assets, hospital collaborators, suppliers and individual employees.

The IAM problem is therefore not only patent ownership. It is the capture of tacit and semi-documented knowledge before it becomes operationally indispensable but legally untraceable.

Without an IAM process, Siemens risks losing trade-secret protection, underclaiming patentable inventions, failing to identify background/foreground assets in collaborations, weakening licensing opportunities and creating internal uncertainty about who controls which asset.

The Board should approve a cross-divisional IAM database for the next-generation SOMATOM programme. The database should identify technology assets, creators, owners, IPRs, trade-secret status, contractual encumbrances, data sources, responsible teams and commercial relevance. It should also distinguish background, sideground and foreground assets in R&D collaborations.

2.5.7 Board-level conclusion

Ranked in order of cumulative legal and strategic exposure, the five priority areas are:

1. MDR / AI Act convergence – because market access depends on an integrated evidence architecture for the medical device and AI system.
2. Clinical evidence, PMS and model drift – because AI-enabled performance must remain safe and valid after market placement.
3. Health-data governance – because lawful and representative data is both a legal precondition and a competitive input.
4. Cybersecurity and hospital-network integration – because the product is a connected node in critical healthcare infrastructure.
5. IP and trade-secret control in cross-divisional R&D – because next-generation value lies in software, data, know-how and system integration as much as in hardware patents.

The Board should endorse these priorities as the basis for the 2026–2027 legal and regulatory workplan.

2.6 Organisational implications for Siemens' legal function

2.6.1 From compliance review to compliance-by-design

The compliance architecture described above cannot be operated through ex post legal review. In the next-generation SOMATOM programme, legal requirements are embedded in product decisions. Intended-purpose wording affects MDR classification. Dataset selection affects AI Act conformity. Data-flow design affects GDPR role allocation. Connectivity architecture affects cybersecurity responsibility and market leverage. Software-update processes affect continuing conformity. IP capture affects future licensing and competitive position.

Compliance-by-design therefore means more than involving legal early. It means translating legal requirements into product-development artefacts: classification memos, dataset provenance

files, update impact assessments, hospital contract modules, AI evidence files, cybersecurity interface assessments and IAM records.

Legal should be present at product-development gates, including concept approval, intended-purpose definition, data-source approval, clinical-validation planning, cybersecurity architecture review, software-release approval and post-market monitoring review.

2.6.2 Capability gaps

The next-generation product exposes several capability gaps.

First, Siemens needs stronger AI governance capability: the ability to translate AI Act obligations into product-team procedures, evidence requirements, monitoring processes and customer-facing instructions.

Secondly, Siemens needs data-protection engineering capability: not only legal GDPR advice, but the ability to understand data flows, anonymisation limits, federated learning, access controls, retention and dataset provenance.

Thirdly, Siemens needs stronger standards literacy inside legal. Regulatory affairs may understand ISO and IEC standards, but legal must be able to assess how standards interact with legal obligations, notified-body expectations and liability exposure.

Fourthly, Siemens needs cybersecurity contracting capability: the ability to translate technical security architecture into customer terms, supplier obligations, remote-access rights, incident-response duties and audit rights.

Lastly, Siemens needs IAM capability across the product lifecycle. This includes invention capture, trade-secret identification, employee know-how mapping, data-asset tagging, software ownership and background/foreground allocation.

2.6.3 Proposed operating model

The recommended operating model is product-centred rather than discipline-centred.

Siemens should establish a product legal squad for the next-generation SOMATOM programme. This squad should include or have direct access to regulatory legal, data protection, AI governance, cybersecurity, IP/IAM, contracting and public-procurement expertise. It should be embedded in the product programme and accountable for compliance-by-design.

At group level, Siemens should centralise specialist competence in MDR/AI Act strategy, AI governance, data-governance architecture, cybersecurity legal strategy, IP/IAM and template contracting. These areas require consistency across products and markets.

Local counsel should remain responsible for jurisdiction-specific issues: public procurement, local healthcare administration, national authority contacts, local customer negotiation, labour law and national implementation of EU obligations.

The model should operate through matrix reporting. Product legal squads should report to both product leadership and group legal. This protects independence while ensuring practical relevance.

A central component of this operating model should be a Board-level product legal-governance repository (hereafter the product repository). The repository should function as the authoritative internal record for active development projects, products currently on the market and discontinued products that remain relevant for post-market surveillance, liability, cybersecurity, documentation or customer-support purposes.

The repository should not be designed as passive file storage. It should be structured around products and development projects. For each product or project, authorised users should be able to access the relevant legal, technical and compliance materials in one place: intended-purpose documentation, classification memoranda, MDR technical documentation, AI Act evidence files, GDPR role assessments, DPIAs, data-flow maps, cybersecurity assessments, post-market surveillance material, software-update records, supplier documentation, customer-contract modules, IP records, trade-secret classifications and IAM information.

Access should be governed by role-based permissions. The system should make relevant information available to the legal, regulatory, technical and commercial teams that need it, while preventing unnecessary access to sensitive IP, trade secrets, personal-data documentation or commercially confidential material. The objective is therefore not unrestricted transparency, but controlled organisational memory.

Ownership of the product repository should sit jointly with Group Legal and Regulatory Affairs, with day-to-day governance shared between those two functions. Product teams should be responsible for maintaining project-level information under defined governance rules, but the repository itself, the access architecture and the document templates should be owned at group level. This division ensures that the repository operates as legal-and-regulatory infrastructure rather than as a product-team archive.

The repository should also support project-level editing and document generation. If designed around the relevant regulatory frameworks, the system can guide product teams to enter the information needed for MDR, AI Act, GDPR, cybersecurity and IAM compliance. Over time, that information can be used to generate or populate the documents required to demonstrate compliance: classification memoranda, data-provenance records, DPIA inputs, AI evidence files, cybersecurity assessments, supplier checklists and update-impact assessments.

This would make the legal function more effective and reduce the risk of fragmented documentation. It would also discipline the product-development process itself. Engineers, product managers and commercial teams would be prompted to consider intended purpose, data use, cybersecurity, IP capture and compliance consequences before design decisions are locked in. The repository would therefore operate not only as a documentation archive, but as a proactive compliance-by-design tool.

2.6.4 Immediate implementation measures

The following measures should be implemented immediately.

(i) The Board should mandate an integrated MDR / AI Act workstream with authority to create the combined evidence architecture and engage the notified body.

(ii) Siemens should establish a centralised product legal-governance repository covering active development projects, marketed products and discontinued products that remain relevant for PMS, liability, cybersecurity, customer support or documentation purposes. The repository should be structured by product and project, with role-based access controls and project-level editing rights.

(iii) The repository should contain, or link to, the key compliance and asset-management materials for each product: intended-purpose documents, classification memoranda, technical documentation, AI evidence files, data-flow maps, GDPR role assessments, DPIAs, cybersecurity assessments, PMS records, software-update records, supplier files, customer-contract modules, IP records and trade-secret classifications.

(iv) Siemens should configure the repository so that compliance information entered at project level can be reused to generate or populate standard legal and regulatory artefacts, including classification memoranda, dataset-provenance records, DPIA inputs, cybersecurity checklists, AI Act evidence files, IAM records and update-impact assessments.

(v) Siemens should create an intended-purpose review process for myExam Companion and new AI functions. Marketing, user-interface design, instructions for use and technical design should not diverge.

(vi) Siemens should issue data-flow templates separating clinical use, remote service, PMS, AI training and commercial telemetry.

(vii) Siemens should develop standard hospital data-access terms covering GDPR roles, Article 9 processing, PMS cooperation, AI-training use, cybersecurity, software updates and international transfers.

(viii) Siemens should create a software-update legal review process. Updates should be screened for safety, intended-purpose change, AI performance impact, cybersecurity implications, data-processing change and customer-contract effects.

(ix) Siemens should develop a cybersecurity interface classification model. Each interface should be classified as open, restricted, Siemens-certified, proprietary or isolated, with legal and technical justification.

(x) Siemens should establish a cross-divisional IAM register, integrated into the product repository, mapping patents, software, datasets, model-related assets, know-how, inventors, owners, contracts and trade-secret status.

(xi) Siemens should develop supplier and customer contracting playbooks for quality, cybersecurity, regulatory cooperation, data protection, remote service, audit rights, IP ownership and incident response.

2.6.5 Strategic conclusion for the Board

The organisational conclusion is that legal work must be structured around product risk rather than legal disciplines alone. The same product decision may simultaneously affect regulatory classification, AI documentation, data protection, cybersecurity, customer contracts and intellectual-asset strategy. A traditional legal function divided into separate regulatory, commercial, IP and privacy silos cannot manage that convergence effectively.

For the next-generation SOMATOM X.cite, the legal function should therefore operate as a governance function embedded in product development. Its role is to make the product legally developable, certifiable, sellable, serviceable, updateable and commercially defensible over time. This conclusion also forms the basis for Part III of this report, where the future company lawyer is analysed as a governance architect rather than a back-office reviewer.

3 Part II – Drafting the Technology License Agreement with Bargeddie Technologies Ltd.

3.1 Transaction context and strategic rationale

3.1.1 The licensed technology and business opportunity

Bargeddie Technologies Ltd. (BTL) has approached Siemens Healthineers with a view to obtaining a licence to United States patent No. 9 842 720, entitled X-ray tube unit, and the associated know-how concerning electric-discharge tubes, X-ray-tube technique and tube units. The commercial purpose, as expressed in the first meeting recorded in Appendix E of Case 2B, is to enable BTL to move from being a component supplier of X-ray subsystems to becoming an end-product manufacturer in the non-destructive industrial-testing market, where the technology has applications distinct from medical imaging.

Two facts inform the legal-object characterisation of the transaction. First, the patent alone is not sufficient to enable BTL: implementation requires substantive know-how that is not embodied in the patent specification. Second, this know-how is precisely the kind of asset that is most easily lost through informal disclosure and most difficult to recover through ex post legal remedy. These two facts shape much of what follows.

3.1.2 Strategic rationale for licensing out

Three considerations support an out-licensing decision in principle. First, the technology has limited strategic value in the medical-imaging core business of Siemens Healthineers, where the patent has been used as a building block for higher-value diagnostic platforms; non-destructive industrial testing is a complementary, non-core application. Second, an out-licence to BTL generates incremental revenue from a portfolio asset that is otherwise under-monetised. Third, well-structured licensing positions Siemens as the technology source in a new application domain, with the prospect of capturing improvements through a grant-back mechanism.

The strategic logic is consistent with the broader intellectual-asset-management framework developed: technology that is non-strategic in one market may be highly strategic in another, and licensing is the legal instrument by which the value across markets is monetised without diluting the core business.

3.1.3 Principal risk of entering into the licence

Against the strategic rationale, six categories of risk must be acknowledged. The first is competitor risk: BTL may, after licence expiry or through retained know-how, compete in

markets contiguous to the licensed field, including the medical-imaging market if field-of-use restrictions are inadequate. The second is technology-leakage risk: know-how, once disclosed, cannot be recalled, and the durability of trade-secret protection depends on the contractual architecture. The third is know-how-dependency risk: BTL is currently incapable of implementing the technology without Siemens assistance, but the duration and intensity of that assistance shape the cost base of the transaction.

The fourth is improvements-control risk: improvements developed by BTL may erode Siemens' technological position if they are not captured by grant-back. The fifth is financial risk: an unduly back-loaded royalty regime exposes Siemens to BTL's commercial success, which is uncertain. The sixth is territory and sublicensing risk: an over-broad territorial grant or unrestricted sublicensing right transfers commercial control over the technology to BTL, with limited remedy available to Siemens short of termination.

3.1.4 Preliminary strategic recommendation

It is recommended that Siemens proceed with the BTL transaction only on the basis of (i) a fully executed non-disclosure agreement before any further substantive technical disclosure; (ii) a field-of-use licence narrowly limited to non-destructive industrial testing; (iii) staged territorial scope, beginning with the United States and expanding upon demonstration of commercial performance; (iv) royalty-bearing financial terms supported by minimum annual payments and milestone payments; (v) a strict grant-back of improvements and tight improvement-control; and (vi) contractually allocated regulatory, quality and trade-secret-compliance obligations on BTL. The remainder of Part II develops this position.

3.2 Legal object: defining and controlling the licensed assets

3.2.1 Patent rights

United States patent No. 9 842 720 is the formal legal object of the transaction. The licensed scope must be defined by reference to the patent claims, the territorial limits of the patent (which on the present record is granted only in the United States), the field of use to which the licence is restricted, and the term of the licence (which cannot meaningfully exceed the residual life of the patent). Equivalent national patents in other jurisdictions, if any, must be enumerated; where the patent is not granted, related know-how, not patent rights, is the operative legal object in that territory.

Patent maintenance obligations remain with Siemens as patentee; the licence agreement should however regulate cooperation in respect of prosecution and enforcement, including the right of

Siemens to control enforcement actions and the duty of BTL to provide reasonable assistance and information. These considerations are operationalised in Clause 13 of the draft below.

3.2.2 Know-how and trade secrets

Know-how is, in this transaction, the more commercially valuable legal object. It comprises documented production techniques, process parameters, materials specifications, testing protocols and undocumented engineering experience held by Siemens personnel. The legal characterisation of this know-how as a trade secret under Directive (EU) 2016/943 and the Swedish Lag (2018:558) om företagshemligheter requires that the information is secret, has commercial value because it is secret, and is subject to reasonable steps to maintain its secrecy. The licence agreement is itself one of those reasonable steps.

Three drafting consequences follow. First, the licensed know-how must be identified with sufficient specificity to support enforcement, while remaining flexible enough to accommodate the iterative nature of technology transfer. The definition adopted in Clause 2 below is by reference to a Schedule listing documented know-how, complemented by a category-based catch-all for undocumented engineering know-how transferred in the course of performance. Second, residual-knowledge clauses, which immunise the licensee against inadvertent retention of information by departed personnel, must be drafted with care: an unrestricted residuals clause is in substance a perpetual royalty-free licence. Third, the trade-secret-protection regime must remain in force after termination, since the loss of secrecy is irreversible.

3.2.3 Improvements

Improvements raise the central legal-object problem of the transaction. Three categorical questions must be answered. Who owns improvements developed unilaterally by BTL during the term? On what terms does Siemens obtain access to such improvements? What is the consequence if BTL chooses to assign or to sublicense its improvements?

The internal strategic position taken is that Siemens shall obtain 100 per cent control over improvements. In commercial practice, this translates either into Siemens ownership of all improvements (an aggressive position that BTL will likely resist) or into BTL ownership with a non-exclusive, royalty-free, worldwide grant-back to Siemens, including the right of Siemens to sublicense (a defensible compromise). The draft in Clause 10 below adopts the latter approach with audit and notification obligations sufficient to give Siemens visibility into BTL's development pipeline.

3.2.4 Boundary problem

Each party will bring to the transaction technology developed independently before the effective date (background intellectual property) and will, during performance, develop new technology (foreground intellectual property). The licensed technology is a defined subset of Siemens background; everything else of Siemens remains reserved. BTL's background remains its own. The boundary between these three categories must be operative throughout the lifetime of the agreement, not merely at signing.

The legal-object architecture is therefore: (i) Siemens background, of which the licensed patent and licensed know-how form a delimited subset to which a licence is granted; (ii) Siemens foreground developed during the term, retained by Siemens and outside the licence unless separately negotiated; (iii) BTL background, retained by BTL and outside the transaction; and (iv) foreground developed by BTL during the term, owned by BTL but subject to the grant-back of Clause 10. This architecture is the conceptual backbone of the clause draft in Clause 5.

3.3 Legal subject: structuring the collaboration between Siemens and BTL

3.3.1 BTL as licensee and potential future competitor

The licence relation positions BTL not merely as a consumer of Siemens technology but as a co-actor in a new application market for that technology. BTL's strategic intention, expressed in the first negotiation meeting, is to evolve from component supplier to full product-solution manufacturer in non-destructive testing. This change of role is legally significant: the licensor is, in effect, equipping a future competitor.

Two consequences follow for the structuring of the legal-subject relation. The field-of-use restriction must operate as a firm boundary between the licensed application (non-destructive testing) and Siemens' core markets (medical imaging and adjacent industrial diagnostic applications), and must be defended both by definitional clarity and by post-term obligations. The collaboration governance – joint steering, technical committees, information flows – must be calibrated to deliver effective technology transfer without creating an open channel through which Siemens commercial intelligence can be acquired.

3.3.2 Knowledge-transfer governance

Technology transfer is performed through documented deliverables (specifications, manuals, drawings, source where applicable) and through personnel-mediated transfer (training sessions, on-site support, secondments). The contractual architecture must regulate both. Documentary deliverables are listed in a transfer schedule and are delivered against acknowledgements that

bring them within the confidentiality regime. Personnel-mediated transfer is governed by clean-team arrangements, by named-personnel access lists, by access-control requirements at the receiving facility and by reciprocal training obligations under non-disclosure terms.

The transfer is finite. The agreement should specify when knowledge transfer is deemed complete, what documentary acceptance procedure terminates it, and how subsequent technical assistance is procured (typically on a fee-bearing time-and-materials basis). Without a defined end point, knowledge-transfer obligations create an open-ended cost base for Siemens.

3.3.3 Secrecy and information-flow architecture

A non-disclosure agreement executed before substantive technical disclosure is not a procedural formality, it is the legal precondition for preserving the trade-secret status of the licensed know-how. Three legal functions of the NDA must be distinguished. First, the NDA imposes contractual confidentiality on BTL and on its representatives, which is enforceable in damages and injunctive relief independently of trade-secret status. Second, the NDA evidences the 'reasonable steps' that Directive (EU) 2016/943 (Article 2(1)(c)) and Lag (2018:558) om företagshemligheter (3 §) require the holder of the trade secret to have taken in order to preserve protection. Third, the NDA structures the pre-contractual exchange: it defines what may be disclosed, by whom, to whom, for what purpose and for how long, and it allocates the consequences of the negotiation failing.

The risks of disclosing without an NDA are correspondingly serious. First and most fundamentally, the trade-secret status of the information may be lost. Once a court accepts that the holder failed to take reasonable steps to maintain secrecy, the information falls out of the protected category, and remedies under the Directive and the Swedish statute become unavailable; recovery of secrecy is, in practice, impossible. Second, contractual remedies in damages may be unavailable or limited to the doctrine of culpa in contrahendo, which under Swedish law provides at most reliance-interest protection and not expectation damages, and which is in any event unsuited to the protection of information assets. Third, the absence of an NDA leaves the dispute about the scope of permitted use to be reconstructed from emails, meeting notes and witness recollection, with very poor evidentiary outcomes. Fourth, BTL is itself exposed: in the absence of contractual scoping, BTL faces the risk of allegations of misuse that it cannot defend by reference to clear permitted-use parameters.

The NDA in the present case should contain, at minimum: a wide definition of confidential information including oral and visual disclosures; a permitted-purpose clause limited to the evaluation and negotiation of the licence; a term of confidentiality of not less than five years from the date of last disclosure (and indefinite for material that remains trade-secret); explicit

injunctive-relief language; a return-or-destruction obligation at the end of the evaluation; and a no-licence clause confirming that no licence is granted by virtue of disclosure under the NDA. The NDA should be governed by Swedish law and the parties should accept the jurisdiction of the Stockholm District Court for any disputes, or alternatively arbitration under the Stockholm Chamber of Commerce.

The Case 2B materials record BTL's apparent reluctance to enter into an NDA. This reluctance is itself a red flag and is to be treated as a precondition for any further substantive engagement. The negotiation strategy below treats the NDA as a non-negotiable threshold rather than as a tactical concession.

3.3.4 Governance bodies

The licence contemplates a multi-year collaboration during which technical, commercial and compliance issues will inevitably arise. The agreement should therefore not rely only on ordinary breach-and-remedy mechanisms. It should establish an internal governance structure capable of managing the relationship while it is ongoing. This is particularly important because the transaction is not a simple patent licence. BTL requires knowledge transfer, technical assistance and continuing access to Siemens-controlled know-how. The legal relationship must therefore organise not only the parties' formal rights, but also the practical cooperation through which the licensed technology is implemented.

The agreement should establish a steering committee composed of an equal number of senior representatives from each party. Its function should be to oversee the commercial relationship, monitor performance against milestones, review royalty and reporting issues, approve or reject proposed territory expansions, and address strategic questions that cannot be resolved at operational level. The steering committee should not, however, have authority to amend the agreement or expand the licence scope unless such amendment is made in writing by authorised signatories of both parties. This limitation is important because informal committee decisions may otherwise be relied upon later as evidence that Siemens accepted a broader field of use, wider technical assistance obligation, or more permissive sublicensing structure.

In addition to the steering committee, the agreement should establish a technical committee. Its role should be narrower and more operational: to coordinate technology-transfer deliverables, monitor implementation issues, document training sessions, handle technical questions, receive improvement notifications, and ensure that access to Siemens know-how remains limited to authorised personnel. The technical committee should also maintain records of what information has been disclosed, when, to whom and for what purpose. This is important from a trade-secret

perspective, since Siemens must be able to show that reasonable steps were taken to preserve the secrecy and controlled dissemination of its know-how.

The agreement should also contain an escalation procedure. Operational disputes should first be handled by the technical committee. If unresolved within a defined period, they should be escalated to the steering committee. If the steering committee cannot resolve the issue, the matter should be escalated to senior executives of both parties before formal dispute resolution is triggered. This staged procedure has two advantages. First, it allows technical and commercial disagreements to be solved by those closest to the relationship before they become legal disputes. Secondly, it creates a written record showing that the parties attempted to preserve the collaboration before initiating adversarial proceedings.

Disputes that cannot be resolved through the internal governance structure should be referred to arbitration rather than ordinary court litigation. Arbitration is preferable in this context for several reasons. The transaction concerns technically complex subject matter, including patent rights, X-ray tube technology, know-how transfer, confidentiality obligations, improvement rights and field-of-use restrictions. An arbitral tribunal can be composed of arbitrators with experience in international technology licensing and complex commercial disputes, which is likely to produce a more commercially and technically informed process than ordinary litigation. Arbitration also offers procedural flexibility, confidentiality and international enforceability, which are particularly valuable where the dispute may concern trade secrets or commercially sensitive technical information.

The arbitration clause should therefore provide for final settlement under the Rules of the Arbitration Institute of the Stockholm Chamber of Commerce, with Stockholm as the seat of arbitration, Swedish law as the governing law and English as the language of the proceedings. However, the arbitration clause should include a carve-out allowing Siemens to seek interim or injunctive relief before a competent court where necessary to protect confidential information, trade secrets, intellectual property rights or to prevent unauthorised use of the licensed technology. This carve-out is essential because the value of trade secrets may be destroyed before a final arbitral award is rendered. In such cases, Siemens must be able to act immediately to prevent disclosure or misuse.

This structure creates a coherent dispute-resolution ladder: technical committee, steering committee, senior executive escalation, arbitration, and emergency court relief where necessary. It preserves the collaborative nature of the licence while ensuring that serious disputes can be resolved effectively and confidentially.

3.3.5 Competition-law perimeter and the TTBER

The licence operates within a competition-law perimeter that conditions every substantive clause of Part II. The doctrinal foundation is Article 101(1) of the Treaty on the Functioning of the European Union, which prohibits agreements between undertakings that may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market. Technology-transfer agreements are capable of falling within that prohibition because they allocate technology, fields of use, territories and downstream commercial conduct between independent undertakings.

Commission Regulation (EU) 2026/877 of 16 April 2026 (the "Technology Transfer Block Exemption Regulation" or "TTBER") gives effect to Article 101(3) TFEU for that category of agreement. The Regulation entered into force on 1 May 2026 and replaces Regulation (EU) No 316/2014, which expired on 30 April 2026. Under Article 10 of the new Regulation, agreements concluded under Regulation 316/2014 benefit from a transitional period until 30 April 2027; the BTL transaction, however, is a new agreement and is therefore drafted directly under the 2026 regime.

Where the conditions of the Regulation are satisfied, the agreement is presumptively exempt from the Article 101(1) prohibition. The TTBER operates as a safe harbour rather than as a positive licence: falling outside the safe harbour does not render an agreement automatically void, but it removes the presumption and exposes the agreement to case-by-case analysis under Article 101(3), with the parties bearing the burden of justification. The drafting objective in this Part is therefore to remain within the safe harbour wherever possible and, where this is not possible, to ensure that the agreement is defensible on its merits.

Three structural elements of the TTBER condition the analysis throughout. First, the safe harbour is conditional on the parties' market shares falling below defined thresholds – a combined 20 per cent for agreements between competing undertakings and an individual 30 per cent for each party in agreements between non-competing undertakings (Article 3 TTBER). Second, hardcore restrictions listed in Article 4 – including restrictions on the licensee's ability to determine its prices, certain output limitations, allocation of markets or customers, and restrictions on the licensee's ability to exploit its own technology or to conduct independent research and development – cause the agreement to fall outside the safe harbour as a whole. Third, excluded restrictions listed in Article 5 – including exclusive grant-backs and assignments of improvements or new applications of the licensed technology, and no-challenge clauses without a corresponding termination right – fall outside the safe harbour but, unlike Article 4 hardcore restrictions, do not contaminate the remainder of the agreement.

The competitor/non-competitor characterisation of the parties is decisive. Under Article 1(1)(n) TTBER, undertakings are competing undertakings where they license out competing technology

rights on the relevant technology market or where they are active, or would on realistic grounds be likely to enter, the relevant product market within a sufficiently short timeframe to impose competitive pressure. The category includes both actual and potential competitors. On the present facts, the parties are not actual competitors: Siemens Healthineers is active in medical imaging and adjacent diagnostic applications, where it holds approximately 22 per cent of the global computed-tomography market and around 35 per cent of the conventional-CT segment in 2025, but it does not sell non-destructive testing equipment. BTL is currently a component supplier of X-ray subsystems and has no end-product activity in either market. The more sensitive question is potential competition on the product market. Appendix C of the internal materials records that Siemens "is not ruling out the possibility of venturing into the NDT product segment in the future", and the same document records that BTL has potential to enter Siemens' core MedTech business. The Article 1(1)(n) test, however, requires entry "on realistic grounds and not just as a mere theoretical possibility" within "a timeframe that is sufficiently short to impose competitive pressure". Appendix C itself qualifies the Siemens position by acknowledging that NDT-grade X-ray products for harsh-environment applications "fall outside the core business activities of Siemens Healthineers", and the decision to commercialise the licensed technology by out-licence rather than by vertical integration is itself evidence that Siemens does not plan timely entry on its own account. BTL's possible expansion into medical imaging is, on the present record, equally theoretical: BTL has no medical-device regulatory history, no MDR conformity-assessment experience and no clinical-evidence base, and entry into medical imaging would require switching costs and lead times far exceeding the timeframe contemplated by the Regulation. On the better view, the parties are therefore non-competitors for the purposes of the TTBER at the time of conclusion of the agreement, and the 30 per cent individual-share threshold applies.

The characterisation should nonetheless be recorded in the transaction file at signing. Article 4(3) TTBER, however, materially reduces the operational consequence of a later change. Where the parties are non-competitors at the time of conclusion of the agreement but become competing undertakings afterwards, Article 4(3) provides that the non-competitor regime in Article 4(2) – and not the stricter competitor regime in Article 4(1) – applies for the full life of the agreement, unless the agreement is subsequently amended in any material respect. The transaction file at signing should therefore record both (i) the non-competitor characterisation, and (ii) the consequence that any material amendment of the agreement following a change in commercial position would trigger reassessment under the more demanding Article 4(1) regime.

The relevant markets for the threshold analysis must then be correctly identified. The CT-imaging market shares cited above are not the relevant markets for the TTBER threshold: they relate to a different product market that lies entirely outside the Licensed Field. Under Article 1(1)(j)–(k) TTBER, the relevant product market is the market for the contract products and their

substitutes – here, NDT X-ray generators and adjacent NDT equipment – and the relevant technology market is the market for the licensed technology rights and their substitutes for use in producing those contract products – here, X-ray tube technology and competing technologies usable in NDT applications. Article 8(d) TTBER, read together with Recital 13, provides that market share on the relevant technology market is calculated on the basis of the combined sales of the licensor and its licensees of contract products incorporating the licensed technology, and that "technologies that have not yet generated sales of contract products should be considered to hold a market share equal to zero". The licensed technology has not yet generated any sales of NDT contract products: Siemens does not sell NDT equipment using this technology, and there are no other existing licensees in the NDT market. Siemens' market share on the relevant technology market for NDT applications is therefore zero by operation of the Regulation, regardless of Siemens' position in the medical-imaging market. On the relevant product market, the total worldwide X-ray generator market is approximately USD 800 million, of which the non-medical segment (which includes but is broader than NDT) accounts for approximately half. Siemens has no commercial presence in the NDT product market and BTL has no end-product presence in any market today. The parties' individual market shares on the relevant product market are accordingly close to zero and well within the 30 per cent threshold. Article 8(e) provides a further three-calendar-year grace period if either threshold is later exceeded.

The applicability of EU competition law over an initial United States-only territory should also be addressed. Article 101 TFEU and the TTBER apply to agreements that may affect trade between Member States and competition within the internal market. The first-stage territorial restriction does not place the agreement outside that scope: BTL is established in the United Kingdom and operates in commercial proximity to EU markets, the staged-territory architecture in Section 3.4.4 contemplates future European Union expansion, and the licensed technology has equivalents and adjacent applications in EU jurisdictions. The agreement is therefore drafted as if EU competition law applies from the outset.

The detailed clause-level consequences of this framework are addressed in the commentary in Section 3.5. The principal load-bearing applications are: the field-of-use restriction (Section 3.5.4); the exclusivity and territorial architecture, in particular the treatment of passive sales (Section 3.5.5); the improvements and grant-back regime (Section 3.5.10); the no-challenge clause and termination right (Section 3.5.15); the prohibition on reverse engineering and on invent-around use of know-how (Section 3.5.16); and the term-and-royalty structure post patent expiry (Section 3.5.21). Each is drafted so as to remain within the TTBER safe harbour or, where the safe harbour is not available, to be defensible on the merits under Article 101(3) TFEU.

3.4 Negotiation strategy

3.4.1 Siemens' negotiation objectives

Siemens' principal negotiation objectives are: control (over field of use, sublicensing, improvements and use of the Siemens name); revenue (an appropriate combination of upfront, milestone, running royalty and minimum payments); market separation (firm preservation of the medical-imaging core market and adjacent industrial diagnostic applications); improvement capture (a robust grant-back); confidentiality (with effective enforcement mechanisms); and auditability (sufficient access to BTL records to verify royalty reporting and field-of-use compliance).

3.4.2 BTL's likely demands

On the basis of the first meeting recorded in Appendix E of Case 2B, BTL can be expected to seek: exclusivity in the non-destructive-testing field; a wide territorial grant including the United States, the European Union (with Germany of particular significance) and China; a right to sublicense or, at minimum, to engage subcontractors; a royalty rate calculated as a percentage of the net selling price of licensed products; broad and continuing access to Siemens know-how, including the personnel of Siemens engineering teams; and a reluctance to be bound by an NDA, particularly one that survives the negotiation phase.

Each of these demands is intelligible from BTL's commercial position but each contains commercial risk for Siemens that the agreement must mitigate. Exclusivity is the most consequential, since it forecloses Siemens from licensing the technology to alternative non-destructive-testing partners; it should be conceded only on the basis of meaningful minimum payments and field-specific carve-outs. Territory should be granted in stages. Sublicensing should be subject to written consent at minimum, and ideally limited to wholly owned subsidiaries. The royalty structure should combine running royalties with minimum payments to bridge the gap between BTL's commercial uncertainty and Siemens' need for predictable revenue.

3.4.3 Siemens' red lines

The following are non-negotiable: no further substantive technical disclosure prior to NDA execution; no unrestricted sublicensing; no use of the licensed technology in the medical field or in any field that the parties have not expressly defined as the licensed field; no uncontrolled improvements; and a minimum-payment floor that protects Siemens' investment in technology transfer regardless of BTL's commercial performance.

3.4.4 Proposed negotiation package

The recommended opening position is: limited exclusivity in the non-destructive-testing field; staged territory beginning with the United States, with the European Union to follow upon demonstrated performance and China to be considered on the basis of an export-control and sanctions assessment; a running royalty in the range of four to six per cent of net sales, an upfront payment of a defined sum, milestone payments at first commercial sale and at defined revenue thresholds, and minimum annual royalties scheduled to escalate; a strict non-exclusive royalty-free grant-back of BTL improvements; audit rights with reasonable notice; and contractually allocated compliance obligations including trade-secret-protection measures, export-control compliance, anti-bribery undertakings and product-safety responsibility for licensed products. The specific financial parameters are reserved to the financial input prepared by the CFO (Appendix F of Case 2B).

3.5 Draft technology license agreement / term sheet with clause commentary

The clauses below are drafted in legal form. They are presented in operative order rather than in the order in which they will appear in the final executed agreement, in which definitions ordinarily precede the grant. Each clause is followed by commentary addressing the legal function of the clause, the assumed facts, the Siemens negotiating position, the principal points of negotiation sensitivity, and the relevant legal-subject / legal-object / compliance lens.

3.5.1 Parties and recitals

Draft clause.

This Technology Licence Agreement (the 'Agreement') is entered into on [Effective Date] between Siemens Healthineers AG, a stock corporation organised under the laws of Germany with its registered office at Henkestrasse 127, 91052 Erlangen, Germany ('Licensor'), and Bargeddie Technologies Ltd., a company incorporated under the laws of Scotland with its registered office at [address] ('Licensee').

Whereas Licensor is the proprietor of United States patent No. 9 842 720, entitled X-ray tube unit, and of substantial associated know-how concerning the design and manufacture of X-ray tube units; whereas Licensee wishes to use such patent and such know-how to develop and to manufacture non-destructive industrial testing equipment; whereas Licensor is willing to grant a licence to such patent and such know-how on the terms set out herein; now therefore the parties agree as follows:

Commentary.

The recitals frame the legal-subject relation: Licensor and Licensee are placed in a defined commercial relationship, and the purpose of the licence is recorded. The purpose statement is interpretive: courts will look to it to construe ambiguous operative clauses. The choice of Licensor entity – here Siemens Healthineers AG rather than Siemens Healthcare AB – is deliberate and reflects the patent holder of record. Internal back-to-back arrangements between Healthineers AG and Healthcare AB will, where necessary, govern revenue allocation within the group.

3.5.2 Definitions

Draft clause.

In this Agreement, the following terms have the following meanings: 'Affiliate' means, in relation to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party, where control means the ownership of more than fifty per cent (50%) of the voting securities or the equivalent power to direct management. 'Licensed Patent' means United States patent No. 9 842 720 and all continuations, divisionals, reissues, re-examinations and extensions thereof. 'Licensed Know-How' means the technical information set out in Schedule 1 and any additional technical information identified in writing by the parties as Licensed Know-How during the term, in each case to the extent owned by or controlled by Licensor and necessary or useful for the manufacture, use or sale of Licensed Products. 'Licensed Technology' means the Licensed Patent and the Licensed Know-How collectively. 'Licensed Field' means the design, manufacture, marketing, sale and servicing of equipment for non-destructive industrial testing, expressly excluding any medical, diagnostic, veterinary or human-imaging application and any application in security screening of persons. 'Licensed Territory' means, in the first instance, the United States of America, with extension to additional territories as agreed in writing pursuant to Clause 4. 'Licensed Product' means any product in the Licensed Field the manufacture, use or sale of which would, but for the licence granted under this Agreement, infringe a Valid Claim of a Licensed Patent or which incorporates Licensed Know-How. 'Improvements' means any invention, modification, enhancement, derivative work or new technical information made or acquired by a party during the term that relates to the Licensed Technology or to the Licensed Products. 'Net Sales' means the gross amount invoiced by Licensee and its Affiliates for sales of Licensed Products to non-Affiliate third parties, less customary deductions for returns, trade discounts and applicable sales taxes. 'Valid Claim' means a claim of an issued and unexpired patent within the Licensed Patent that has not been held invalid by a court or competent authority in a non-appealable decision. 'Effective Date' means the date first written above. 'Term' has the meaning set out in Clause 21.

Commentary.

Definitions are the load-bearing legal-object architecture of the agreement. Three definitional choices are particularly consequential. The definition of Licensed Know-How combines a closed schedule (Schedule 1) with a written-amendment mechanism: this disciplines the boundary of the licensed information without preventing the practical iteration of technology transfer. The definition of Licensed Field is exclusionary as well as inclusive: by expressly listing medical, diagnostic, veterinary, human-imaging and security-screening uses as excluded, Siemens reduces the interpretive scope for boundary disputes. The definition of Licensed Product captures both patent-infringing products and know-how-incorporating products, which is necessary in a hybrid patent-and-know-how licence because the post-expiry use of know-how is otherwise unrestrained.

3.5.3 Grant of licence

Draft clause.

Subject to the terms and conditions of this Agreement, Licensor hereby grants to Licensee a licence under the Licensed Technology to develop, manufacture, have manufactured, use, market, sell, offer for sale and import Licensed Products in the Licensed Field in the Licensed Territory. The licence is non-transferable except as expressly permitted in Clause 21 and is exclusive within the Licensed Field and Licensed Territory subject to Clause 5. The licence granted under this Clause does not extend to any use outside the Licensed Field or outside the Licensed Territory, and any such use shall constitute a material breach of this Agreement.

Commentary.

The grant clause is the operative transfer of contractual permission. Three features deserve attention. First, the bundle of rights granted ('develop, manufacture, have manufactured, use, market, sell, offer for sale and import') is broad enough to support a full manufacturing operation by Licensee. Second, 'have manufactured' permits contract manufacturing without separate consent but does not authorise sublicensing; the distinction is operationally important and is reinforced in Clause 6. Third, the exclusivity is qualified by Clause 5, which reserves to Licensor the right to continue to use the Licensed Technology outside the Licensed Field and outside the Licensed Territory. This is the legal-object boundary protection that gives effect to the strategic position taken in Section 3.1.4.

3.5.4 Field of use and territory

Draft clause.

The Licensee shall use the Licensed Technology exclusively within the Licensed Field. The Licensee acknowledges that the Licensor relies on the field-of-use restriction as a material condition of the licence and that use of the Licensed Technology outside the Licensed Field constitutes both a breach of this Agreement and an infringement of the Licensed Patent. The Licensed Territory may be extended to one or more additional countries upon written agreement of the parties and upon adjustment, as appropriate, of the financial terms in Schedule 2.

Commentary.

Field-of-use clauses operate within the TTBER framework described in Section 3.3.5. Restrictions on the licensee's field of use are permitted in agreements between non-competitors and are not listed as hardcore restrictions under Article 4(2) of Regulation (EU) 2026/877, provided that they are precisely defined; the exclusionary specification in the definition of Licensed Field (medical, diagnostic, veterinary, human-imaging and security-screening uses) is intended to provide that precision. Staged territory has commercial as well as legal logic: it allows Siemens to observe Licensee's performance before extending market exposure, subject to the passive-sales considerations addressed in Section 3.5.5.

3.5.5 Exclusivity and reservation of rights

Draft clause.

The licence granted under Clause 3 is exclusive in the Licensed Field in the Licensed Territory, and accordingly Licensor undertakes not to grant any further licence under the Licensed Technology to any third party for the Licensed Field in the Licensed Territory during the term. All rights not expressly granted to Licensee are reserved to Licensor, including without limitation: (i) the right of Licensor to use and to license the Licensed Technology outside the Licensed Field; (ii) the right of Licensor to use and to license the Licensed Technology outside the Licensed Territory; and (iii) the right of Licensor to continue research, development and use of the Licensed Technology for its own purposes including for Licensor's medical-device business.

Commentary.

Reservation-of-rights clauses appear formalistic but perform substantive work: they confirm that the grant of an exclusive licence in one field does not silently encumber the licensor in adjacent fields. The express reservation in subparagraph (iii) is particularly important for Siemens, since the licensed patent originated as a building block for medical-imaging technology and Siemens must remain free to develop further medical applications without Licensee consent or notification. Without this clause, an exclusive licensee may seek to argue that downstream Licensor activity competes with the licensee's reasonable expectations.

A further word on the competition-law treatment of the exclusivity grant. Exclusivity in a licence between non-competitors is, in itself, permitted within the TTBER safe harbour: Articles 4 and 5 of Regulation (EU) 2026/877 contain no generic prohibition on exclusivity, and the licensor's undertaking not to license third parties in the Licensed Field in the Licensed Territory is therefore unproblematic so long as the parties remain non-competitors and the threshold conditions of Article 3 are satisfied. The competition-sensitive questions arise instead in respect of the *consequences* of exclusivity for downstream sales flows. Under Article 4(2)(b) TTBER, restrictions on the territory into which, or the customers to whom, the licensee may *passively* sell the contract products are hardcore restrictions, subject to narrowly drawn carve-outs that include the protection of an exclusive territory or exclusive customer group reserved for the licensor. The staged-territory architecture proposed in Section 3.4.4 must therefore be operated with care: when the Licensed Territory is extended in due course to the European Union, or when Siemens grants a parallel licence in respect of any territory not yet allocated to BTL, the agreement should not purport to restrict BTL's passive sales from the United States or any other Licensed Territory into those reserved or subsequently-allocated territories. Active-sales restrictions may be imposed within the limits of Article 4(2)(b)(i); passive-sales restrictions are hardcore save in the carve-out scenarios listed in the Regulation and would cause the agreement as a whole to fall outside the safe harbour. This distinction must be carried forward when Schedule 2 (territorial scope and financial terms) is amended on each future expansion.

3.5.6 Sublicensing

Draft clause.

Licensee shall not sublicense any rights granted under this Agreement without the prior written consent of Licensor, such consent not to be unreasonably withheld in the case of wholly owned Affiliates of Licensee. Any permitted sublicensee shall be bound by terms no less protective of Licensor than the terms of this Agreement, and Licensee shall remain primarily liable for the performance of any sublicensee. Licensee shall provide Licensor with a true copy of each sublicence within thirty (30) days of execution. The right to engage contract manufacturers under Clause 3 ('have manufactured') does not constitute sublicensing for the purposes of this Clause, provided that any such contract manufacturer is bound by confidentiality obligations equivalent to those imposed on Licensee under this Agreement.

Commentary.

Sublicensing is one of the most leverage-sensitive clauses in any licence. A broad sublicensing right transfers commercial control to the licensee; a strict prohibition may make the licence commercially impracticable. The compromise here is consent-based with an Affiliate carve-out,

supported by flow-through obligations and primary-liability retention. The distinction between 'have manufactured' and sublicensing is drawn explicitly to prevent the licensee from using the contract-manufacturing right as a back-door for de facto sublicensing.

3.5.7 Technology transfer and technical assistance

Draft clause.

Licensor shall, during the period commencing on the Effective Date and ending eighteen (18) months thereafter (the 'Transfer Period'), provide to Licensee the technology-transfer deliverables specified in Schedule 3 and shall make reasonably available, at Licensee's request, up to two hundred (200) person-days of technical assistance through named Licensor personnel, on the terms set out in Schedule 3. Licensee shall pay Licensor for technical assistance in excess of two hundred person-days, and for technical assistance after the Transfer Period, on the time-and-materials basis set out in Schedule 3. All technology transfer shall be conducted under the confidentiality obligations of Clause 8 and through such clean-team and access-control measures as the parties' Technical Committee shall determine.

Commentary.

The technology-transfer clause is the operative mechanism through which the legal-subject collaboration is performed. The clause must be definite: a Transfer Period of defined duration, a documented set of deliverables, a capped allocation of personnel-mediated assistance, and a fee mechanism for excess. Without these elements, the Licensor is exposed to indefinite obligations and unrecouped costs. The reference to clean-team and access-control measures is the mechanism through which trade-secret protection is operationalised during transfer and is the principal channel through which the 'reasonable steps' standard of the Trade Secrets Directive is satisfied.

3.5.8 Confidentiality and trade-secret protection

Draft clause.

Each party (the 'Receiving Party') shall maintain in confidence all Confidential Information of the other party (the 'Disclosing Party') and shall not use or disclose such information except as expressly permitted by this Agreement. 'Confidential Information' means all technical, commercial, financial and other information disclosed by the Disclosing Party to the Receiving Party in connection with this Agreement, whether in writing, orally, visually, electronically or otherwise, and whether or not marked as confidential, but excludes information that the Receiving Party can demonstrate (i) was lawfully in its possession without confidentiality

obligation before disclosure; (ii) is or becomes publicly known through no breach of this Agreement; (iii) was lawfully received from a third party not under a confidentiality obligation to the Disclosing Party; or (iv) was independently developed without use of or reference to the Confidential Information of the Disclosing Party. The Receiving Party shall protect the Confidential Information of the Disclosing Party using at least the same degree of care it applies to its own confidential information of similar importance and in any event no less than a reasonable degree of care. The confidentiality obligations under this Clause shall remain in force for ten (10) years after the expiration or termination of this Agreement, save that for Licensed Know-How that constitutes a trade secret the obligations shall remain in force for so long as such information retains its trade-secret character.

Commentary.

The confidentiality clause performs three distinct functions. First, it imposes contractual confidentiality enforceable in its own right. Second, it forms part of the 'reasonable steps' Siemens must take to preserve trade-secret status under Directive (EU) 2016/943 and the Swedish Trade Secrets Act. Third, the tiered duration – ten years generally, indefinite for trade-secret know-how – prevents the unintentional expiration of trade-secret protection by way of an unduly short contractual term. The standard exclusions are drafted in a manner that requires the Receiving Party to bear the burden of proof, which is the appropriate allocation for an information-asset-protection regime.

3.5.9 Non-solicitation of key personnel

Draft clause.

During the term of this Agreement and for a period of twenty-four (24) months thereafter, neither Party shall, without the prior written consent of the other Party, directly or indirectly solicit for employment, recruit, hire or engage as a consultant any individual who is or has been employed by, or engaged as a consultant to, the other Party at any time during the term, and who has had access to Confidential Information or to Licensed Know-How in the course of performance of this Agreement. The restriction in this Clause shall not apply to: (i) the engagement of any individual who responds to a general advertisement or recruitment campaign not specifically targeted at the other Party's personnel; (ii) the engagement of any individual whose employment or consultancy with the other Party terminated of its own accord at least six (6) months prior to the engagement; or (iii) the engagement of any individual with the prior written consent of the other Party, such consent not to be unreasonably withheld where the individual's role with the engaging Party will not involve activities that compete with the other Party's business.

Commentary.

Non-solicitation clauses are particularly important in this transaction because the technology-transfer mechanism in Clause 7 is partly personnel-mediated: Licensor personnel will work alongside Licensee personnel during the Transfer Period, and Licensee will inevitably become aware of which individuals hold the operative engineering know-how. A 24-month tail is at the upper end of what Swedish courts will sustain in a commercial context; if the clause is challenged, the existence of a Confidential-Information nexus and the carve-outs are the features that protect enforceability. The general-advertising and own-initiative carve-outs are essential, since clauses without them are routinely struck down as restraints of trade.

3.5.10 Improvements and grant-back

Draft clause.

Improvements made by Licensee during the term shall be the property of Licensee. Licensee hereby grants to Licensor a perpetual, irrevocable, worldwide, non-exclusive, royalty-free, sublicensable licence under such Improvements to develop, manufacture, use, market, sell and import products in all fields and territories. Licensee shall notify Licensor in writing of each Improvement within sixty (60) days of its conception and shall provide Licensor with all information reasonably necessary to enable Licensor to practise the Improvement. Improvements made by Licensor during the term shall be the property of Licensor and shall be included within the Licensed Know-How (and, in the case of patentable Improvements, within the Licensed Patent) for the purposes of this Agreement.

Commentary.

This clause embodies the most aggressive control element of the legal-object architecture. The structure adopted – Licensee ownership coupled with a non-exclusive royalty-free worldwide grant-back, with sublicensing rights for the Licensor – gives Siemens the practical benefit of Licensee development without imposing the ownership-transfer or exclusive-licence-back position that Article 5(1)(a) TTBER treats as an excluded restriction. The notification obligation is the operative mechanism: without it, the grant-back is unenforceable in practice. The non-exclusive structure of the grant-back is not merely a negotiating compromise; it is the structural choice required by the competition-law perimeter described in Section 3.3.5. Article 5(1)(a) of Regulation (EU) 2026/877 broadened the scope of the previously-existing excluded restriction: it now applies to any direct or indirect obligation on the licensee to grant an exclusive licence or to assign rights, in whole or in part, to the licensor or to a third party designated by the licensor in respect of the licensee's own improvements to, or new applications of, the licensed technology. The previous "severability" limitation, under which exclusive grant-backs of non-severable improvements remained within the safe harbour, has not been carried forward. The position is

therefore now clear: any exclusive grant-back, whether of severable or non-severable improvements, falls outside the safe harbour. A non-exclusive grant-back, by contrast, remains within the safe harbour and is the structure adopted here. The further design choices – the obligation to notify each Improvement, the licensor's right to sublicense the grant-back, and the licensor's right to use the Improvement in all fields – are not restricted by Article 5, since they operate on the licensor side of the grant-back rather than on the licensee's ability to exploit its own Improvements. The licensee remains free to use, license and exploit its Improvements in the Licensed Field and elsewhere; what the agreement secures is parallel access for the licensor. The reciprocal inclusion of Licensor Improvements within Licensed Know-How preserves the commercial value of the licence over time.

3.5.11 Financial terms

Draft clause.

In consideration of the licence granted under this Agreement, Licensee shall pay to Licensor: (a) a non-refundable upfront payment of [EUR amount] within thirty (30) days of the Effective Date; (b) milestone payments of [amounts] upon the achievement of the milestones set out in Schedule 2; (c) a running royalty of [percentage]% of the Net Sales of Licensed Products, payable quarterly within forty-five (45) days of the end of each calendar quarter; and (d) minimum annual royalties of [amount in year 1, escalating per Schedule 2], creditable against running royalties accrued in the same calendar year. All amounts are exclusive of value-added tax and other applicable taxes, which shall be added at the rate prevailing on the date of invoice. Late payments shall bear interest at the rate of three per cent (3%) above the Swedish Riksbank reference rate from the due date until payment.

Commentary.

The financial architecture of the licence is a stacked instrument. The upfront payment compensates Siemens for the technology-transfer investment and for the option value foregone by entering an exclusive arrangement. The milestone payments align the parties on commercial performance and capture value as it is created. The running royalty preserves an interest in Licensee's long-term performance. The minimum royalty addresses the principal Siemens risk in an exclusive licence – that the licensee fails to commercialise, denying Siemens both running royalties and the opportunity to license elsewhere. Net Sales is defined narrowly to prevent erosion through customary deductions exploited by aggressive accounting.

3.5.12 Records, audit and reporting

Draft clause.

Licensee shall maintain complete and accurate records of all Licensed Products manufactured, used and sold by Licensee and its Affiliates in such form as is necessary to verify the calculation of royalties and the compliance of Licensee with this Agreement. Licensor may, not more than once per calendar year, upon thirty (30) days' written notice and through an independent auditor of recognised international standing bound by appropriate confidentiality obligations, audit such records. If the audit discloses an underpayment of more than five per cent (5%) for the audited period, Licensee shall reimburse the reasonable costs of the audit and shall pay the underpaid amount with interest at the rate set out in Clause 11.

Commentary.

Audit rights translate the confidentiality of the licensee's accounting records into a Licensor right of verification. The independent-auditor mechanism resolves the tension between Licensee's legitimate confidentiality interest and Licensor's interest in royalty verification: the auditor sees the data, the Licensor sees the conclusion. The five-per-cent threshold for cost-shifting deters frivolous audit requests while preserving Licensor's ability to seek verification on reasonable grounds.

3.5.13 Intellectual-property prosecution, maintenance and enforcement

Draft clause.

Licensor shall, at its own cost, maintain the Licensed Patent in force during the term of this Agreement. Licensor shall have the sole right, but not the obligation, to prosecute applications and to enforce the Licensed Patent against third-party infringers. If Licensor declines to enforce the Licensed Patent against an infringer in the Licensed Field and in the Licensed Territory within ninety (90) days of receipt of a written request from Licensee, Licensee shall have the right to bring such enforcement action at its own cost, in which case any recovery shall be applied first to the costs of the action and the balance shall be allocated [as set out in Schedule 4]. Each party shall reasonably cooperate with the other in any such enforcement action.

Commentary.

Patent enforcement is the legal mechanism by which the exclusive licence retains its economic value. The clause preserves Licensor's primary right of enforcement, since uncoordinated enforcement actions across territories and fields are damaging to the patent portfolio, while providing Licensee with a fall-back step-in right in respect of infringements in its Licensed Field

and Licensed Territory. The cost-and-recovery mechanism aligns incentives without ceding control of the patent.

3.5.14 Cooperation in defence of the Licensed Patent

Draft clause.

If either Party becomes aware of any actual, threatened or suspected challenge by a third party to the validity, enforceability or ownership of the Licensed Patent, or of any other proceeding capable of materially affecting the Licensed Patent ("IP Challenge"), that Party shall promptly notify the other Party in writing, providing such information about the IP Challenge as is then available to it.

Licensor shall have the conduct of the defence of any IP Challenge and shall bear its own costs of such defence. Licensee shall provide such reasonable cooperation as Licensor may request, including by making available, on reasonable notice and at Licensor's expense in respect of out-of-pocket costs, relevant personnel for the giving of evidence, technical documentation, internal assessments and proprietary data necessary or useful for the defence, and by participating in joint legal and technical analysis where the Parties so agree.

Neither Party shall, in connection with any IP Challenge, take any action – whether by way of public statement, private communication, withdrawal of evidence, support for a third party or otherwise – that is materially adverse to the validity, enforceability or ownership of the Licensed Patent. No Party shall settle, withdraw or compromise any IP Challenge in a manner that materially affects the rights of the other Party under this Agreement without the prior written consent of that other Party, such consent not to be unreasonably withheld.

The obligations of cooperation, non-adverse conduct and joint settlement approval set out in this Clause shall survive termination of this Agreement for so long as the Licensed Patent remains in force in any jurisdiction.

Commentary.

The clause complements the offensive enforcement architecture in Clause 13, which addresses Licensor's right to bring infringement proceedings against third parties, by adding a corresponding defensive architecture. Two features merit attention. First, the cost allocation is conventional: Licensor, as patentee, bears the defence cost, but Licensee bears its own internal cost of cooperation, with out-of-pocket expenses reimbursable. This is the inverse of the unusual position taken in the Wintermute model, in which the licensee carries the full defence cost; that position would be unsustainable on a Siemens-perspective licence-out. Second, the prohibition on materially-adverse conduct, paired with the joint-settlement requirement, prevents Licensee

from indirectly undermining the patent during a defensive proceeding – either by supporting a parallel third-party challenge or by accepting a narrowing settlement that compromises Licensor's broader patent position. The survival clause is necessary because the patent's residual life will, in many cases, exceed the term of the licence.

3.5.15 No-challenge of the Licensed Patent

Draft clause.

Licensee shall not, during the term of this Agreement, directly or indirectly (i) challenge the validity, scope, enforceability or ownership of the Licensed Patent, whether in opposition, revocation, invalidity, declaratory or other proceedings before any court, patent office or competent authority; (ii) assist, fund, instruct or otherwise support any third party in bringing such a challenge; or (iii) procure that any Affiliate of Licensee does any of the foregoing. Nothing in this Clause shall preclude Licensee from raising the validity or enforceability of the Licensed Patent by way of defence to an infringement action brought against it by Licensor, nor shall this Clause apply to the extent that any prohibition would be void under applicable competition law, including Article 101 of the Treaty on the Functioning of the European Union as interpreted in light of Commission Regulation (EU) 2026/877. In the event that Licensee, or any Affiliate of Licensee, brings or supports any challenge falling within sub-paragraphs (i) or (ii), Licensor shall have the right, exercisable on written notice, to terminate this Agreement with immediate effect and without prejudice to any accrued rights and remedies.

Commentary.

The clause performs two distinct functions. First, it preserves the integrity of the licensed patent against the most damaging form of attack – namely an attack mounted from inside the licence relation by the very party best placed to do so. Second, it converts what would otherwise be a non-exempt restriction under competition law into an exempt termination right. Article 5(1)(b) of the Technology Transfer Block Exemption Regulation permits a no-challenge obligation in an exclusive licence only if the licensor retains the right to terminate; the second sentence and the termination right at the end of the clause are drafted in light of that requirement. The carve-out for raising invalidity as a defence is included because that line of conduct is not within the legitimate reach of a no-challenge clause and cannot, as a matter of mandatory law, be precluded.

3.5.16 Prohibition on reverse engineering and on invent-around use of know-how

Draft clause.

Licensee shall not, and shall procure that its Affiliates, contract manufacturers and any permitted sublicensees shall not, reverse-engineer, decompile, disassemble, dismantle or otherwise attempt to derive the underlying design, structure or composition of the Licensed Technology or of any Licensed Product, save to the extent that such conduct is expressly required by mandatory law and cannot lawfully be excluded by contract.

During the term, Licensee shall not use any Licensed Know-How for the purpose of designing, developing or producing any technology or product that is functionally equivalent to or substitutable for the Licensed Technology in the Licensed Field. For the avoidance of doubt, nothing in this Clause shall prevent Licensee from carrying out independent research and development using technology that is not Licensed Know-How, provided that such research and development is conducted without recourse to or reliance on Licensed Know-How.

Commentary.

The first paragraph is a conventional reverse-engineering prohibition with the mandatory-law carve-out necessary in jurisdictions that protect reverse engineering for interoperability or research purposes; Article 5 of Directive 2009/24/EC on the legal protection of computer programs is a representative example. The second paragraph addresses the invent-around problem at a level that is enforceable: it restricts Licensee from leveraging the disclosed know-how to produce substitutable technology, but does not impose a blanket non-compete on Licensee's independent development efforts. A blanket non-compete would fall foul of Article 5(2) of the Technology Transfer Block Exemption Regulation and would expose the Agreement to broader competition-law risk. The narrower formulation here protects the trade-secret value of the Licensed Know-How without overreach.

3.5.17 Compliance obligations

Draft clause.

Licensee shall, in the manufacture, use and sale of Licensed Products: (a) comply with all applicable laws and regulations, including in respect of product safety, electromagnetic compatibility, radiation safety, export control, sanctions and anti-corruption; (b) not use the Licensed Technology in any application within the medical, diagnostic, veterinary, human-imaging or security-screening fields; (c) implement and maintain appropriate technical and organisational measures to protect the confidentiality of the Licensed Know-How, consistent with the standard required to maintain trade-secret protection under Directive (EU) 2016/943; and (d) impose, by written agreement, equivalent obligations on its Affiliates, contract manufacturers and any permitted sublicensees. Licensee shall promptly notify Licensor of any

allegation of non-compliance and shall cooperate with Licensor in the investigation and remediation thereof.

Commentary.

This clause is the principal vehicle for compliance as contractual risk allocation. The pass-through structure (subparagraph (d)) is essential: it extends Siemens' control of the trade secret into the Licensee's supply chain, without which the chain of custody is broken at the first contract-manufacturing interface. The express prohibition of medical-field use (subparagraph (b)) reinforces the field-of-use restriction at the compliance layer and creates a contractual link between an out-of-field use and the consequences set out in Clause 21.

3.5.18 Quality control and regulatory responsibility

Draft clause.

Licensee is solely responsible for the regulatory compliance of Licensed Products placed on the market by Licensee, including the obtaining of all necessary approvals, certifications and registrations. Licensor makes no representation that the Licensed Technology is suitable for any particular purpose or that the manufacture or sale of Licensed Products will not infringe the intellectual-property rights of any third party. Licensee shall implement a quality-management system appropriate to the manufacture of Licensed Products. The use of any Licensor trade mark, trade name or other indicia of origin in connection with Licensed Products is prohibited save with the prior written consent of Licensor.

Commentary.

Two distinct points are addressed in this clause. The first is the allocation of regulatory responsibility for Licensed Products: as the manufacturer of those products under the applicable product-safety regimes, Licensee bears the regulatory burden, and Licensor bears no derivative regulatory liability. The second is the protection of the Licensor's reputational interests through the trade-mark prohibition: even where the Licensed Products incorporate Siemens technology, they are not Siemens products and should not be marketed as such.

3.5.19 Representations and warranties

Draft clause.

Licensor represents and warrants that, as at the Effective Date, (i) it is the lawful proprietor of the Licensed Patent; (ii) it has the right to grant the licence granted under this Agreement; and (iii) it has no actual knowledge of any third-party claim that the Licensed Patent is invalid or

unenforceable. Save as expressly set out in this Clause, Licensor makes no representation or warranty in respect of the Licensed Technology, including without limitation in respect of validity, enforceability, non-infringement, merchantability or fitness for a particular purpose, and all such representations and warranties are expressly disclaimed.

Commentary.

Representations and warranties allocate ex ante information risk. Licensor's representations are narrow – title, right to grant, no actual knowledge of invalidity – and exclude the broader assurances that Licensee may seek (no infringement of third-party rights, performance to specifications, commercial viability). For know-how-heavy licences, the broad assurance regime is incompatible with the inherently uncertain quality of know-how, and the restrictive approach taken here is industry-standard.

3.5.20 Indemnities and limitation of liability

Draft clause.

Licensee shall indemnify and hold harmless Licensor and its Affiliates from and against all losses, damages, liabilities and expenses arising out of or in connection with (i) any product-liability claim relating to Licensed Products manufactured, used or sold by Licensee or its Affiliates; (ii) any breach by Licensee of Clause 17 (Compliance Obligations) or Clause 8 (Confidentiality); and (iii) any use of the Licensed Technology outside the Licensed Field or outside the Licensed Territory. Save in respect of (a) liability for death or personal injury caused by negligence, (b) liability for fraud or fraudulent misrepresentation, (c) liability under the indemnity in this Clause, (d) liability for breach of confidentiality under Clause 8, and (e) any other liability that cannot lawfully be limited or excluded, the aggregate liability of each party to the other under or in connection with this Agreement shall not exceed [an amount linked to fees paid in the preceding twelve months]. In no event shall either party be liable for indirect, special, incidental or consequential damages, save in respect of the matters specified in subparagraphs (a) to (e).

Commentary.

Liability allocation is the most heavily negotiated commercial clause in technology licences. The structure here protects Licensor on the product-liability axis (where the manufacturer of Licensed Products bears the risk), preserves the integrity of the compliance and confidentiality regimes by carving them out of the liability cap, and respects mandatory law by carving out non-excludable liabilities. The cap should be calibrated by reference to the financial parameters of the deal, with running-royalty-based formulations being preferable to fixed amounts for long-term agreements.

3.5.21 Term and termination

Draft clause.

This Agreement shall enter into force on the Effective Date and shall continue, on a country-by-country basis, until the later of (i) the expiry of the last-to-expire Valid Claim of the Licensed Patent in such country or (ii) ten (10) years from the Effective Date, after which the licence under the Licensed Know-How in such country shall become non-exclusive and royalty-free, save in respect of Licensed Know-How that retains its trade-secret character, in respect of which the obligations of Clause 8 shall continue. Either party may terminate this Agreement on written notice if: (a) the other party commits a material breach of this Agreement that, if capable of remedy, is not remedied within sixty (60) days of written notice; (b) the other party becomes insolvent, enters into voluntary or compulsory liquidation, has an administrator or receiver appointed over its assets, or is the subject of analogous proceedings; or (c) a change of control occurs in respect of the other party in favour of a Competitor of the terminating party. Licensor may further terminate this Agreement on written notice in the event of any use of the Licensed Technology outside the Licensed Field.

Commentary.

The term structure addresses the persistent legal-object problem of know-how licences: patent expiry. A licence that terminates with the patent leaves the Licensee free to use the know-how royalty-free, which is inefficient for the Licensor. A licence that continues royalties beyond patent expiry on the know-how is, however, vulnerable to challenge under competition law. The compromise here is a defined term (10 years or last-to-expire patent, whichever is later), after which the know-how licence becomes royalty-free but the confidentiality regime continues. The change-of-control termination protects Siemens against an indirect acquisition of the licensed technology by a strategic competitor.

The defined-term structure also responds to a specific competition-law concern about post-expiry royalties on hybrid patent-and-know-how licences. The position established by the Court of Justice in Genentech v. Hoechst (Case C-567/14, judgment of 7 July 2016) is that running royalties may continue to be paid beyond the expiry of the licensed patent provided the licensee is free to terminate the agreement: in such a case the consideration is properly characterised as paid for the know-how rather than for the (expired) patent monopoly, and the arrangement is not, on that ground alone, contrary to Article 101 TFEU. That position interprets the Treaty directly and is unaffected by the entry into force of Regulation (EU) 2026/877. The drafting here is more conservative: at the defined term, the know-how licence becomes non-exclusive and royalty-free, while the confidentiality regime continues to operate for so long as the Licensed Know-How

retains its trade-secret character. This places the post-expiry position clearly within the TTBER safe harbour without requiring reliance on the Genentech line, and avoids the more difficult evidential question of how a continuing royalty would be valued in the absence of the patent monopoly. The protection of the trade-secret status of the Licensed Know-How after termination is moreover supported directly by Article 2(2) TTBER, which provides that the block exemption applies in respect of know-how for as long as the know-how remains secret.

3.5.22 Effects of termination

Draft clause.

Upon termination of this Agreement, (i) all licences granted to Licensee shall terminate, save that Licensee may sell off existing inventory of Licensed Products for a period of six (6) months upon payment of running royalties at the rate set out in Clause 11; (ii) Licensee shall, in addition to its other obligations under this Clause, return to Licensor or, at Licensor's election, destroy all copies of the Licensed Know-How in its possession or under its control in any form, together with all materials, tools, equipment, jigs, fixtures, manuals, training records and other items in its possession or under its control that contain, embody or enable the practice of the Licensed Know-How. Licensee shall, within thirty (30) days of the effective date of termination, deliver to Licensor a written certificate signed by a senior officer of Licensee confirming that such return or destruction has been completed in full, identifying with reasonable specificity the items returned or destroyed, and confirming that no copies, derivations or extracts have been retained save for one (1) archival copy held by Licensee's legal department for the sole purpose of evidencing compliance with this Agreement; (iii) Clauses 8 (Confidentiality), 10 (Improvements – to the extent of accrued grant-back rights), 14 (Defence), 13 (Enforcement – to the extent of accrued rights), 20 (Indemnities and Limitation of Liability) and 23 (Governing Law and Dispute Resolution) shall survive; and (iv) all payment obligations accrued prior to termination shall remain due.

Commentary.

The clause extends the existing return-or-destroy obligation in two operationally significant directions. First, it expressly captures materials and tools that enable the practice of the Licensed Know-How – manuals, jigs, training records – and not merely documentary copies. Second, the certification is made specific: the senior-officer signature, the identification of items, and the limitation of retained copies to a single archival legal copy convert what is often an empty formality into a meaningful evidentiary act. The archival-copy carve-out is included because Licensee will, as a practical matter, need to be able to demonstrate compliance in any subsequent

dispute, and an absolute destruction obligation creates an enforceability problem rather than solving one.

3.5.23 Governing law and dispute resolution

Draft clause.

This Agreement shall be governed by and construed in accordance with the laws of Sweden, without regard to its conflict-of-laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods. Any dispute, controversy or claim arising out of or in connection with this Agreement shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce in accordance with its Rules. The seat of arbitration shall be Stockholm, Sweden. The language of the arbitration shall be English. Nothing in this Clause shall prevent a party from seeking injunctive or other interim relief from any court of competent jurisdiction.

Commentary.

The combined choice of Swedish law, Stockholm seat and SCC arbitration reflects three considerations. First, Swedish law is the home jurisdiction of the Licensor entity acting on behalf of the Siemens Healthcare AB group, although the Licensor entity in the recitals is German for patent-title reasons. Second, the SCC is an internationally respected institution with substantial experience in technology disputes. Third, the injunctive-relief carve-out preserves the ability to seek urgent interim measures from a national court, which is essential where trade-secret protection is at stake and the speed of national-court interim relief exceeds that available in arbitration.

3.5.24 Boilerplate provisions

Draft clause.

This Agreement, together with its Schedules, constitutes the entire agreement of the parties in respect of its subject matter and supersedes all prior agreements, understandings and communications. No amendment shall be effective unless in writing and signed by an authorised representative of each party. No waiver of any provision shall be effective unless in writing and shall not constitute a waiver of any subsequent breach. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect, and the parties shall negotiate in good faith a substitute provision having the closest possible commercial effect. Neither party shall be liable for any failure or delay in performance due to circumstances beyond its reasonable control. Notices shall be given in writing to the addresses

set out in the recitals or to such other address as a party may notify in writing. This Agreement may be executed in counterparts, including by electronic signature.

Commentary.

The boilerplate clauses are not, despite the name, perfunctory. Entire-agreement clauses preclude reliance on pre-contractual representations and discipline the pre-contractual exchange to the four corners of the agreement. Severability ensures that a single clause's invalidity does not unravel the transaction. Force-majeure protects against unforeseeable performance interruption. Notices clauses are operationally critical at the point of breach. Each merits attention proportionate to its legal function.

3.6 Part II synthesis

3.6.1 The license as collaboration between legal subjects

The agreement structures Siemens and BTL as collaborating legal subjects through the recitals (which record the joint purpose), the technology-transfer clause (which performs the knowledge transfer through documented deliverables and personnel-mediated assistance), the steering and technical committees (which provide ongoing governance) and the audit and notification mechanisms (which sustain the information symmetry necessary for an exclusive licence). The collaboration is bounded – through the field-of-use restriction, the sublicensing constraint and the confidentiality regime – but it is collaboration nevertheless.

3.6.2 The technology as a managed legal object

The licensed technology is constituted as a manageable legal object through the definitional architecture (Licensed Patent, Licensed Know-How, Improvements, Licensed Field, Licensed Territory, Licensed Product), through the technology-transfer schedule (which delimits the documentary perimeter of the know-how) and through the boundary clauses (which preserve the distinction between background, foreground and licensed technology). The trade-secret-protection regime in Clauses 8 (Confidentiality) and 17 (Compliance Obligations) ensures that the legal-object character of the know-how is maintained against the entropy of disclosure.

3.6.3 Compliance as contractual risk allocation

Compliance obligations are not parked in a single clause but are distributed across the agreement: the trade-secret-protection obligations in Clauses 8 (Confidentiality) and 17 (Compliance Obligations), the regulatory-responsibility allocation in Clause 18 (Quality Control

and Regulatory Responsibility), the indemnity for breaches of compliance and confidentiality in Clause 20 (Indemnities and Limitation of Liability), the field-of-use enforcement in Clauses 4 (Field of Use) and 17 (Compliance Obligations), and the pass-through structure in Clause 17(d) that extends the compliance regime into Licensee's supply chain. The cumulative effect is that compliance is contractually allocated to the party best able to bear it, and that Siemens' residual exposure is bounded.

3.6.4 Recommendation to the Board before negotiation with BTL

The Board is recommended to authorise the legal division to enter into the BTL negotiation on the basis of (i) the precondition that the NDA in Schedule 0 be executed before any further substantive disclosure; (ii) the opening positions on field, territory, exclusivity and sublicensing set out in Section 3.4; (iii) the financial parameters submitted separately by the CFO; and (iv) the clause architecture set out in Section 3.5. Departure from these positions in the course of negotiation shall be reported to the Board through the Head of the Legal Division and shall, in respect of red-line departures, require prior Board approval.

4 Part III – The Future Role of the Company Lawyer

The reflection in this part is grounded in the SOMATOM X.cite compliance analysis and in the BTL licence drafting, and it draws conclusions about the competencies, the organisation and the strategic posture that the company lawyer must possess in a multinational MedTech group active on technology-convergent markets.

4.1 What the case shows about the future company lawyer

4.1.1 SOMATOM X.cite: legal work inside product development

The Part I analysis demonstrates that, for a product such as the next-generation SOMATOM X.cite, legal compliance cannot be discharged at the placing-on-the-market stage by way of documentation review. The MDR, AI Act and GDPR obligations are produced at the design stage; they are evidenced by artefacts that must be developed in parallel with the technical workstream; and they continue throughout the lifecycle of the product through post-market monitoring, software updates and incident response. The company lawyer who is to operate effectively in this environment must therefore be present in product-development meetings, in clinical-evidence planning, in data-flow design and in software-release governance – not in a passive review capacity, but as a co-designer of the legal architecture of the product.

4.1.2 BTL license: legal work inside value creation

The Part II analysis demonstrates that licensing is not a transactional matter of papering a commercial decision taken elsewhere. The legal-subject and legal-object work – defining the technology, characterising the know-how, structuring the field of use, calibrating the grant-back, allocating the compliance burden – is itself the value-creation work of the transaction. The boundary between commercial strategy and legal design dissolves: there is no commercial strategy in a technology licence that is not legal, and no legal architecture that is not commercial.

4.1.3 The common denominator

Across the two domains, the company lawyer is no longer a function that is consulted; the company lawyer is a function that participates. Legal work is, in this account, a constitutive element of product strategy, asset management and business-model design – not an external constraint upon them. This is the foundation of the role reconstruction developed in the remainder of this Part.

4.2 Necessary competencies

4.2.1 Substantive legal competence

The substantive base must extend across regulatory law (MDR, AI Act, GDPR, NIS2, product liability), intellectual-property law (patent, copyright, design, with growing weight on the patent-software interface), trade-secret law (Directive (EU) 2016/943 and national implementations), licensing and contracting (technology licences, processor agreements, supply contracts, hospital agreements), data-protection law, cybersecurity law, AI governance, public procurement (for direct customer contracts with public authorities), and competition law (particularly in licensing). Depth in each is unattainable; familiarity in all is essential, and the company lawyer must know where the limits of competence lie.

4.2.2 Technical and organisational literacy

Technical literacy is necessary but insufficient. The company lawyer must understand the technology tree, the product architecture, the AI lifecycle, the clinical workflow and the data pipeline at a level that supports analytical engagement with the engineering, regulatory and clinical functions. Mere familiarity with terminology will not produce useful legal advice; the lawyer must understand how the technology generates value and how value-generation maps to

legal risk. This is technical competence, not technical literacy, and it must extend to the meta-level question of how technical systems behave in operation.

4.2.3 Contract-design competence

Contracting is the legal medium through which technical and commercial strategy is converted into enforceable obligations. The company lawyer must be able to design contract structures that target the operative commercial and technical questions, not those that import generic templates without close engagement with the underlying transaction. The BTL clause draft in Part II is an example of how a technical understanding of the licensed technology informs the structure of the legal-object architecture, the field-of-use restriction, the technology-transfer mechanism and the improvement-control regime.

4.2.4 Ethical and professional judgment

The company lawyer in a regulated MedTech business bears responsibilities that exceed the duties of an ordinary commercial counsel. Patient safety is at stake in MDR matters; the rights of data subjects are at stake in GDPR matters; the integrity of the regulatory system is at stake in conformity-assessment matters. The lawyer must preserve professional independence in the face of commercial pressure, must escalate ethical issues through appropriate internal channels, and must be willing to refuse work or to record a reservation where compliance and commercial pressure cannot be reconciled. The professional-responsibility dimension of the role grows in proportion to the embedded nature of the function.

4.3 Organising legal work in a multinational group

4.3.1 The problem: fragmented knowledge and group-level assets

The Case 2A material discloses that valuable assets within the Siemens group are distributed across divisions, that visibility into those assets is limited, and that siloing reduces the leverage that can be obtained from them. The legal function inherits this problem in concentrated form: regulatory strategy decisions in one division have consequences for AI-governance posture group-wide; intellectual-asset positions in one subsidiary affect licensing options elsewhere; cybersecurity-incident response in one entity affects NIS2 reporting obligations across the group. Fragmented legal organisation reproduces the fragmentation of the underlying assets.

4.3.2 What should be centralised

Functions where the marginal cost of decentralisation exceeds the benefit of local responsiveness should be centralised: AI governance, given its specialist nature and its policy implications across products; MDR and AI Act regulatory strategy, given the integration challenges discussed in Part I; intellectual-asset management and the maintenance of the asset database; data-governance policy and the framework for lawful provenance of training data; cybersecurity policy and incident management; group-level template contracting (hospital agreements, supplier agreements, processor agreements, licensing templates); and export-control and dual-use compliance where the product crosses into sensitive markets.

4.3.3 What should remain local

Functions where local expertise and local relationships are determinative should remain decentralised: national healthcare-administrative law (which is jurisdictionally specific and operationally interfaces with hospital customers and regulators); labour law (which is national in character and requires local counsel familiarity); public-procurement matters (which depend on national procedural law and authority relationships); market-specific contracting; and the maintenance of local authority contacts in respect of regulatory submissions and inspections.

4.3.4 Coordination mechanisms

Centralisation without coordination produces an ivory tower; decentralisation without coordination produces inconsistency. The recommended coordination mechanisms are: matrix reporting, with product-aligned reporting lines complementing entity-aligned reporting lines; product legal squads embedded in major product programmes and drawing on both central and local expertise; group-level playbooks for recurring transaction types (hospital agreement, licensing, supplier agreement) updated by central specialists; a cross-divisional intellectual-asset-management database; and escalation committees that channel disputes about scope, prioritisation and resource allocation to a defined decision-maker.

4.4 From back-office to strategic decision-making

4.4.1 Why the traditional model fails here

The back-office model of legal practice – the lawyer is consulted by the business, advises on a specific question, returns a memorandum and disengages – fails in the technology-convergent context for three reasons. First, compliance choices shape product design: an AI-architecture choice taken without legal input may foreclose a conformity-assessment route. Second, data-

strategy choices made without legal input may compromise the lawful provenance of training data with consequences that cannot be remediated retrospectively. Third, software-update governance taken without legal input may inadvertently trigger substantial-modification analysis with significant regulatory consequences. The lawyer who is consulted ex post can describe the problem but cannot prevent it.

4.4.2 The embedded company lawyer

The alternative is the embedded lawyer who participates in product-development meetings, in licensing strategy, in product roadmap discussions and in Board-level risk decisions. The embedded lawyer is not an advocate of the legal interest against the business interest; the embedded lawyer designs the legal architecture that makes the business interest legally sustainable. This is the governance-architect role anticipated in Section 4.4.4.

4.4.3 Limits and risks of embedding

The embedded model creates two risks that the traditional model does not. The first is the loss of professional independence: the lawyer who is embedded in a product team may identify too closely with the commercial outcome and may, in consequence, fail to raise compliance concerns with appropriate force. The second is the conflict between speed and compliance: embedded lawyers are placed under pressure to produce answers that match the cadence of product development, which may not be the cadence that the legal question requires. Both risks must be managed through institutional mechanisms – clear reporting lines to a Group Legal function that retains hierarchical independence; documented escalation routes; protected time for legal analysis on questions that warrant it; and a culture in which the recording of a reservation is treated as a professional contribution and not as friction.

4.4.4 Final reflection

The future company lawyer in a multinational MedTech group is best understood as a governance architect. The role is to structure legal subjects (the parties to transactions, the economic operators in regulatory frameworks, the controllers and processors of data) and legal objects (technology, know-how, data, intellectual-property rights, contractual rights) so that the technology developed by the company can be commercialised, controlled and continuously improved within the legal frameworks that govern it. This is constitutive work, not merely advisory work; it produces the legal forms through which technical and commercial activity is possible. The competencies and the organisation discussed above are calibrated to this

conception of the role, and the case work in Parts I and II demonstrates that the conception is not aspirational but operationally necessary.

5 Conclusions and Board recommendations

The recommendations set out below consolidate the conclusions of Parts I, II and III. They are framed in operative form for Board action. The Board is invited to endorse each recommendation in principle and to delegate to the Head of the Legal Division the elaboration of implementation plans and resource allocations.

5.1 Compliance recommendations

(a) Establish an integrated MDR / AI Act compliance workstream for the next generation of the SOMATOM X.cite, with delegated authority to develop the combined technical-documentation file, to engage with the notified body on the combined conformity-assessment pathway, and to coordinate Article 10 AI Act data-quality compliance with GDPR lawful-basis analysis.

(b) Implement an AI post-market monitoring programme designed to detect performance degradation and model drift, integrated with the MDR post-market surveillance plan and with vigilance reporting under both regimes.

(c) Develop a group-level health-data-governance framework addressing the lawful provenance of historical and future training data, the conditions for secondary use of post-market data, anonymisation and pseudonymisation pipelines, hospital-data-access contracting standards, and the conditions for cross-border transfer of training data.

(d) Implement cybersecurity-by-design protocols extending from product engineering through hospital-network integration to remote-service delivery, integrated with NIS2 incident-reporting procedures and with the management-body training and approval requirements of Article 20 of the Directive.

(e) Confirm the appointment and the empowerment of the person responsible for regulatory compliance under Article 15 MDR and of the data-protection officer under Article 37 GDPR, with documented escalation routes to the Head of the Legal Division and to the Board.

5.2 Licensing recommendations

(a) Proceed with the Bargeddie Technologies Ltd. transaction only on the basis of a fully executed non-disclosure agreement covering pre-contract disclosure, with the terms described in Section 3.3.3 and embodied in the form attached as Schedule 0 of the draft.

(b) Enter the negotiation on the opening positions described in Section 3.4.4: field of use limited to non-destructive industrial testing; staged territory beginning with the United States; running royalty supported by upfront, milestone and minimum-annual payments; strict non-exclusive

royalty-free grant-back; consent-based sublicensing; and contractually allocated regulatory, trade-secret and export-control compliance obligations.

(c) Maintain Siemens ownership and control over improvements through the grant-back mechanism in Clause 10 of the draft, with documented notification obligations sufficient to provide Siemens with visibility into Licensee's development pipeline.

(d) Authorise the Head of the Legal Division to execute the Agreement in substantially the form attached, subject to the financial parameters submitted separately by the CFO and subject to escalation of red-line departures for Board approval.

5.3 Organisational recommendations

(a) Centralise group-level competence in AI governance, regulatory strategy, intellectual-asset management, data governance, cybersecurity and template contracting in a dedicated Group Legal centre of excellence reporting to the Head of the Legal Division.

(b) Embed legal counsel in major product-development programmes through cross-functional product legal squads accountable both to product leadership and to the Group Legal centre, with documented compliance-by-design responsibilities at each lifecycle stage.

(c) Develop and maintain a cross-divisional intellectual-asset-management database capturing the technology tree, ownership, encumbrances, licence status and freedom-to-operate assessments for the principal assets of the group.

(d) Issue a group-level contract architecture for the principal recurring transactions in the AI-MedTech business – hospital agreements, supplier agreements, processor agreements, licensing – that operationalises the compliance and intellectual-asset positions described in this report.

(e) Adopt the role description of the company lawyer as a governance architect, as set out in Section 4.4.4, and align the recruitment, training and performance-management frameworks of the legal function accordingly.

(f) Establish a centralised Board-level product legal-governance repository for active development projects, marketed products and discontinued products. The repository should be structured by product and project, subject to role-based access controls, and contain or link to the core legal, regulatory, technical and IAM documentation: intended-purpose records, classification memoranda, MDR technical documentation, AI Act evidence files, GDPR assessments, DPIAs, data-flow maps, cybersecurity assessments, PMS records, update assessments, supplier files, customer-contract modules, IP records and trade-secret classifications.

(g) Configure the repository as a compliance-by-design tool rather than merely as document storage. Product teams should be required to enter structured information on intended purpose, data use, AI functionality, cybersecurity, IP ownership, trade-secret status and supplier/customer dependencies. That structured information should then support the generation of standard compliance artefacts and make project teams aware of legal requirements before product decisions become technically or commercially locked in.

6 Back matter

6.1 Appendix 1 – Compliance Map (clean copy of Section 2.2.7)

(Reproduces the table set out in Section 2.2.7 above.)

6.2 Appendix 2 – Draft Non-Disclosure Agreement (Schedule 0 to the Licence)

[To be drafted in accordance with Section 3.3.3: definition of confidential information; permitted purpose limited to evaluation and negotiation of the licence; confidentiality term of five years from last disclosure (indefinite for trade-secret information); return-or-destroy at the end of evaluation; no-licence-by-implication clause; injunctive-relief language; Swedish governing law and SCC arbitration with carve-out for interim relief from national courts.]

6.3 Appendix 3 – Schedule 1 to the Licence: Licensed Know-How

[Inventory of documented know-how to be enumerated by reference to internal Siemens technical-documentation references, with a category-based catch-all for undocumented engineering know-how transferred during the Transfer Period as set out in Section 3.2.2.]

6.4 Appendix 4 – Schedule 2 to the Licence: Financial Terms

[Upfront payment; milestone payments and triggers; running royalty rate on Net Sales; minimum annual royalties with escalation schedule; tax handling; late-payment interest. Specific figures to be inserted on the basis of the financial input prepared by the CFO (Appendix F of Case 2B).]

6.5 Appendix 5 – Schedule 3 to the Licence: Technology Transfer Deliverables and Technical Assistance

[Documented deliverables, milestones for delivery, acceptance procedure, named personnel for technical assistance, allocation of person-days, time-and-materials rates for excess assistance, clean-team and access-control specifications.]

6.6 Appendix 6 – Glossary of technical and regulatory terms

CT (Computed Tomography);

myExam Companion (AI-based workflow assistant for CT examinations);

CE marking (Conformité Européenne);

GSPR (General Safety and Performance Requirements, Annex I MDR);

PMS (Post-Market Surveillance);

PRRC (Person Responsible for Regulatory Compliance, Article 15 MDR);

DPO (Data Protection Officer);

DPIA (Data Protection Impact Assessment);

MDCG (Medical Device Coordination Group);

EDPB (European Data Protection Board);

NIS2 (Network and Information Security Directive 2);

SCC (Stockholm Chamber of Commerce);

BATNA (Best Alternative to a Negotiated Agreement);

NDT (Non-Destructive Testing); FTO (Freedom To Operate); IAM (Intellectual Asset Management);

TFEU (Treaty on the Functioning of the European Union);

TTBER (Technology Transfer Block Exemption Regulation, Regulation (EU) 2026/877).

Bibliography of References

6.7 Union legislation

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (MDR), OJ L 117/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), OJ L 1689/1.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR), OJ L 119/1.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333/80.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets), OJ L 157/1.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L 2847.

Commission Regulation (EU) 2026/877 of 16 April 2026 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, OJ L 2026/877.

Directive 85/374/EEC of 25 July 1985 concerning liability for defective products; recast by Directive (EU) 2024/2853 (PLD recast), OJ L 2853.

6.8 Swedish legislation

Lag (2018:558) om företagshemligheter.

Patentlag (1967:837).

Cybersäkerhetslag (forthcoming implementation of NIS2).

6.9 Soft-law guidance

MDCG 2019-11, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.

MDCG 2019-16, Guidance on Cybersecurity for Medical Devices.

MDCG 2020-1, Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software.

EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (cited for transferable methodology).

Commission Notice – Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements (2014/C 89/03). [Issued in respect of Regulation (EU) No 316/2014; retained as interpretive material pending re-issuance under Regulation (EU) 2026/877.]

6.10 Standards

ISO 13485:2016 – Medical devices: Quality management systems – Requirements for regulatory purposes.

ISO 14971:2019 – Medical devices: Application of risk management to medical devices.

IEC 62304:2006/A1:2015 – Medical device software: Software life cycle processes.

IEC 62366-1:2015 – Medical devices: Application of usability engineering to medical devices.

IEC 60601-1:2005/A1:2012 – Medical electrical equipment: General requirements for basic safety and essential performance.

IEC 60601-2-44 – Medical electrical equipment: Particular requirements for the basic safety and essential performance of X-ray equipment for computed tomography.

IEC 81001-5-1:2021 – Health software and health IT systems safety, effectiveness and security.

ISO/IEC 42001:2023 – Information technology: Artificial intelligence: Management system.

ISO/IEC 27001:2022 – Information security management systems.

ISO/IEC 27701:2019 – Privacy information management.

6.11 Internal materials (Case 2)

Siemens Healthcare AB / Siemens Healthineers, Case 2A – Group Assignment: Next-generation SOMATOM X.cite (myExam Companion), 2026.

Christoffer Hermansson, Instructions and supporting appendices, Case 2B – Individual Assignment (Appendices A–F), 2026.

United States Patent No. 9 842 720, X-ray tube unit.