Data Protection Impact Assessment		
Nr.	**Questions**	**Answer**
1. General pre-processing analysis		
	Person(s) involved in the pre-process.	*Carlos Meca, Chief Business Officer* *Andrea Corsi, Radiologist* *Thibault Bolin, System Administrator* *Sebastian Vandeput, Data Manager*
	End responsible of this pre-process.	*Carlos Meca, Chief Business Officer*
1.1	Summary description of the system, applications, processes and data involved - as well as the project/initiative	*This DPIA concerns a retrospective data collection trial (medical images and abstraction of medical records) of stage III non-small cell lung cancer (NSCLC) patients. The collected real-world data will be used to explore the value of using advanced imaging analysis from Computerised Tomography (CT) scans, namely radiomics technology, to diagnose, characterise and predict the onset of Interstitial Lung Disease (ILD)/pneumonitis related to an oncological treatment. These developments will enable improvements in patient care and therapeutic pathways. This trial is funded by AstraZeneca, a pharmaceutical sponsor that acts as the Controller for the data processing activities conducted in the context of the study. Data will be collected from serveral sites across Europe (Belgium, France, Ireland, Italy, Poland, Spain), each acting as controllers, separate from one another and from AstraZeneca. AstraZeneca employs Oncoradiomics (hereinafter: Radiomics) to collect and analyze the data on their behalf and in accordance with the Professional Services Agreement between the parties. This agreement includes a Data Processig Agreement (hereinafter: DPA), which defines the instructions under which Radiomics shall process the data for the purpose of the trial.* *Data will be collected after financial contract, DTA and DPA completion. Images will be collected via the SFTP server. The abstract medical records will be collected via a pseudonymized pre-completed xls EDC.* *For a site staff member to upload the images, please see attached 'P-DAT-05 Requesting Access'.* *For details on site uploads (data collection), please see attached 'SFTP data Transfer Guidelines'.* *For details on processing during data transfer, please see attached 'P-DAT-04 Data Collection'.* *For the data lifecycle document, containing at the end the steps for archiving the project and destruction of the data, please see attached 'P-DAT-01 Data Life Cycle'.* *The scope of this DPIA covers the processing activities performed by Radiomics in the context of the retrospective study to collect and analyze data based on AstraZeneca's instructions.*
1.2	What are the expected Test and GO-Live dates for this project	*Sep-24*
1.3	Diagram providing insights into all data flows (across systems/applications and across processes)	*Diagrams can be found in the ref documents of question 1.1*
1.4	Who is responsible and/or accountable for the processing of the personal data.	*As separate data controllers, AstraZeneca and the clinical sites are each responsible for ensuring that the data processing activities they or their processor(s) conduct comply with applicable data protection laws, including the General Data Protection Regulation (GDPR).* *Futhermore, for collecting trial data, each site has to respect the law of their countries in relation to data protection, namely:* *For Belgium: The Law of 30th of July 2018 on the protection of individuals with regard to the processing of personal data.* *For Italy: Legislative Decree 196/2003 is the Italian regulation on data protection and privacy.* *For Spain: Organic Law 3/2018, of 5 December, on the protection of personal data and the guarantee of digital rights.* *For Ireland: Data Protection Act 1998, amended in 2003.* *For France: Law on information technology, files and civil liberties.* *For Poland: Personal Data Protection Act.* *As AstraZeneca's processor, Radiomics must comply with AstraZeneca's instructions. As required under Article 28 GDPR, a Data Processing Agreement (hereinafter: DPA) between the parties will be signed to define the instructions under which Radiomics shall process study data for the purpose of the trial. Radiomics' segmentation team will process all images, overseen by the head of segmentation. The data manager will assure access to data based on the principle of least privileged access. The CBO/PM will oversee all activities in this project. All processes will follow predefined flows in the QMS.*
1.5	Is regular compliance monitoring foreseen throughout the project?	*Yes, by the data manager & CBO.*
2. Personal data in scope		
2.1	Indication of segments/types/roles/categories of data subjects are involved.	*Category of data subjects = patients* *Considering the retrospective and descriptive nature of the study, the study sample size is not based on formal statistical considerations. For model purposes, the study targets 200 patients with a confirmed Interstitial Lung Disease /pneumonitis within 12 months follow-up (expected to meet the duration of treatment and eventual Interstitial Lung Disease diagnosis) and an additional control group of at least 200 patients without any Interstitial Lung Disease /pneumonitis will be collected for a total of 400 patients' data. Data will be collected from several sites in Europe, including Galway . Being a multinational multicentric study, it is not fully known how many datapoints can be acquired for each site. Given the heterogenous nature of the disease, the variability on the diagnostic and the low prevalence of the adverse event, maximum number of data subjects will be collected at each data site to maximise chances of project success.*
2.2	Indication of personal data processed of persons under 16 years of age, with/out a lawful representative (guardian)?	*No children are involved in this study.*
2.3	Indication (best estimation) of total personal data collected	*~400 patients*
2.4	Is the personal information collected by "my" organisation directly or collected in an indirect way.	*All data collected will be transferred from clinical sites to Radiomics for processing following financial agreement, DTA and DPA via SFTP and pseudonymized xld EDC.*
3. Categorisation of personal data (incl. sensitive (special categories) data)		
3.1	Which categories of personal data are collected/processed?	*Data collected in this study includes (i) medical images (CT) from patient visits to treatment, and (ii) clinical data, such as year of birth, weight, smoking, status of the disease, specific past medical events, lab results, treatment plan. Such data concerning health is classified as sensitive data (special categories of personal data) under Article 9 GDPR. Therefore, study data will be pseudonymized at the source after conciliation of image and clinical data, transfer and QC.*
3.1.2	Technical and business Metadata/Data fields	*AI for health and medical field.*
3.2	Is there a legal ground (or exception for processing sensitive (special categories) data?	*Yes, data collection from patients by the sites relies on a legal obligation to provide quality healthcare and establish patient records (Article 6.1, c) GDPR) and the necessity of providing health care or treatment to patients (Article 9.2, h) GDPR).* *Data processing by Radiomics and AstraZeneca in the study context constitutes further processing, which is compatible with the initial purpose of providing patient care. Indeed, this trial aims to gain deeper insights into lung cancer diagnosis and treatment. This implies that for the secondary use of patient data for this trial can rely on the same legal grounds as the initial data collection.*
3.3	Which types and categories of data subjects are involved?	*Patients*
4. Objectives with regards to the processing personal data.		
4.1	For which main purposes is personal data used?	*The collected real-world data will be used to explore the value of using advanced imaging analysis from Computerised Tomography (CT) scans, namely radiomics technology, to diagnose, characterise and predict the onset of Interstitial Lung Disease (ILD)/pneumonitis related to an oncological treatment.* *Segmentations, features extractions, AI models are the core processes provided by Radiomics applied on scan images.* *These developments will enable improvements in patient care and therapeutic pathways.*
4.2	Is the data collected required for/aligned with the purposes?	*Yes, data collection is proportionate to the purposes of the study. Data will only be used for the purposes of this trial, as defined in the DTA/DPA.*
4.3	Is personal data used which was previously gathered?	*Retrospective data will be used. All of the enrolled sites' ethical committee checked that the purposes of this project comply with the legal bases outlined by the GDPR and national laws.*
5. Legal ground(s) for processing the data		
5.1	Is the processing of personal data required for the execution of a contract between the data subject and the controller?	*No*

5.2	Was consent requested/obtained from data subjects?	*Based on the current circumstances, consent will not be requested or obtained from data subjects for the following reasons:* *1) Low number of living data subjects: The estimated percentage of patients still alive is between 10% and 15% on average, as data collection will start from patients diagnosed in March 2023 and go back to at least January 2016. Specifically, around 20% of patients diagnosed in March 2023 may still be alive, while this figure may drop to less than 2% for those diagnosed in January 2016. For deceased patients, consent can no longer be obtained, as GDPR requires consent to come from the data subject themselves, not their family members. Additionally, GDPR only applies to the processing of personal data relating to living individuals.* *2) Italian regulatory framework: Recent updates to Italian law (Article 110 of the Privacy Code) state that consent is not required when informing data subjects is impossible or involves disproportionate effort. In this case, many data subjects are deceased, making it impossible to obtain consent directly. For living data subjects, the data used for the research is not directly identifiable, as direct identifiers are removed before being passed on to Radiomics. If data subjects were to be contacted, AstraZeneca, as the data controller, would need to re-identify them, which is unnecessary in this context and could lead to a violation of data subjects' privacy.* *Given these considerations and the implementation of the security measures outlines in Section 11 of this DPIA, it is justified to proceed without consent under the exemptions provided in the updated regulations and the guidelines issued by the Italian Data Protection Authority for processing health data for research purposes.*
5.2.a	If consent was given by the data subject, is the solution/are the solutions and processes designed in a way that allow the data subject to withdraw his/her consent easily?	*N/A*
5.3	In case special personal data (sensitive/special categories data) is processed, is there a legal exception or valid ground to process this type of data?	*Yes. Imaging data and health care data used in hospitals is collected in order to provide health care or treatment to patients (Article 9.2, h) GDPR). As explained above, the processing of this data in the context of the study can rely on the same legal basis since it is compatible with the initial purposes of providing patient care.*
6. Description of IT and process landscape & changes		
6.1	Where is the personal data stored, processed, integrated and analysed?	*Imaging and clinical data will be stored on GCP (Google Cloud Platform) during the transfer and then directly on local servers of Radiomics.*
6.2	Is any personal data exchanged to a third party (processor)?	*Yes, this is documented in the DTA. AstraZeneca, as main sponsor, is the controller and Radiomics is the processor of the data.*
6.3	Is personal data available to another party (e.g. IT services, cloud services,...)?	*Data will be transferred via SFTP through a virtual machine stored on cloud. GCP is also used for the backup (preventing loss of data).*
6.3.1	Is a contract setup with the processor/controller?	*A DPA is signed between AstraZeneca and Radiomics, and a DTA is signed between these parties and each clinical site.* *Radiomics ensures required contracts are made with any controller and/or processor, and all subcontractors, including description of the process, roles and responsibilities, type of data processed, duration of the contract and project and retention period.*
7. Informing data subjects about the storage/processing/exchange of their personal data (transparency in processing)		
7.1	How is the data subject informed about the storage or processing/exchange/profiling/storage of its personal data?	*Study data is pseudonymized in such a way that Radiomics cannot directly identify the data subjects, hence the exception of Article 11 GDPR applies. According to this exception, when personal data has been pseudonymized to the extent that direct identification of the data subject (patients in this case) is no longer feasible, there is no requirement to process additional information solely for the purpose of informing individuals about the use of their data for research purposes. In fact, this would require disproportionate and counter-productive efforts. Therefore, data subjects will not be informed about the further processing of their data in this context.*
8. Qualitative aspects (DQ, data minimization, proportionality, subsidiarity)		
8.1	Can the purpose also be obtained by using less personal data (data minimization)	*No. The study collects only purely relevant information. A combination of imaging data and minimal clinical data is needed to achieve the goal of this trial.*
8.2	Can the purpose of the initiative be obtained with data anonymization?	*Images and clinical data for this retrospective data collection trial will be pseudonymized at the site, with the identification key never leaving the site and deleted after transfer and QC passed (preventing re-identification of patient data).* *Data will be initially uploaded by the personnel at the site to a secured cloud server based in Europe (Google Cloud in Belgium) in a secure and encrypted way (Secure File Transfer Protocol: sftp). Data in the cloud will be subject to a Personal Identification Information (PII) check by Radiomics data privacy manager, not directly involved in the project. Upon approval from the data privacy manager, images will only then be saved on the Radiomics server (based in Belgium).* *The types of data that will remain after the PII check are: imaging (CT scans), post-processed imaging (e.g., segmentation masks), post-processed imaging features (e.g., segmentation features), clinical (e.g., patient demographics, medication history).*
8.3	Is a process in place to assure the involved personal data has (and keeps) the right level of quality and integrity?	*Data will be collected as per study protocol eligible patients and imaging data with a stated minimal quality. Collected data will be analyzed as per Professional Services Agreement, which include a DPA, and DTA.*
9. Retention and deletion of personal data (incl. data minimization)		
9.1	Is a retention period defined for each category of personal data (within it's context)?	*Yes. All data which is used for the purposes of the project will be stored for the duration of the study and archived as per ICH GCP regulations. After this period, all data will be destroyed.* *Radiomics has also an information security management system to ensure that data is correctly protected.* *Data is encrypted during the transfer and at rest on Radiomics' internal servers.* *Accesses are limited to the project team, and there are logs of accesses and changes (preventing unauthorized access, data breaches).*
9.2	How is personal data deleted (hard delete) when data retention periods end?	*When data needs to be deleted, the method of shredding is used. Overwriting is used to destroy the portion of the disk where data is still there, even after you delete it. This is done to avoid a third party to access data using advanced techniques. The command used for shredding will consequently overwrite 3 times, replacing data with other random data. Once it is done, the data is finally destroyed.*
10. Ability to adhere to the rights of the data subject.		
10.1	Is the system/process/integration,... designed to be able to adhere to the rights of the data subject?	*Yes, Radiomics' storage system and processes define data access, rectification and deletion flows. Radiomics' ticketing system is used for oversight and tracking.* *As stated in the DTA, the sites and AstraZeneca agree that the responsibility for complying with Data Subject Requests falls to the party that received such request in respect of the personal data held and under the responsibility of that party as Data Controller. AstraZeneca and the sites agree to cooperate and provide reasonable assistance to each other to help (1) complying with applicable Data Protection Laws, (2) complying with Subject Requests and (3) responding to any other queries or complaints from Data Subjects.* *As AstraZeneca's processor, Radiomics will notify AstraZeneca within 5 business days if they receive any request or complaint from a data subject. Radiomics will also provide support in addressing and complying with such requests.*
11. Data protection and security		
11.1	Security measures in place to secure the personal data against intrusion, theft, loss or inappropriate access/storage or processing of data	*Data import/export procedure* *Any transfer of sensitive material between a third-party and Radiomics must happen through a secure and encrypted virtual machine on Google Cloud Platform services based in the European Union (Belgium). This method will be used to receive data from clinical sites.* *Data privacy measures* *Once transferred to Radiomics, data will be controlled with a series of checks. The first one consists in a personal identifiable information (PII) check to ensure that Radiomics will work on pseudonymised data. If received data does not comply with the de-identification check, Radiomics will proceed to the necessary de-identification steps and proceed with the rest of data processing.* *Data encryption measures* *Data will be stored and managed internally on on-premises and off-premises servers. Off-premises servers are hosted by Google Cloud Platform services based in the European Union (Belgium). Data will be encrypted at transfer.*

		Measures to reduce risk of inappropriate data access/data breaches *Any data potentially containing personal information going through Google's infrastructure must be encrypted to ensure Google and any potential intruders are unable to read the data content.* *In addition, Radiomics has internal processes to ensure data access follows the least privilege principple and only allow project members to access the data. Isolated environements are used when processing of data to follow the data segregation principle per project.* *Data deletion* *At the end of the study, the storage instances located on Google Cloud Platform and data on-premises servers will be deleted or archived following ICH GCP regulations.* *Monitoring of connection & accesses* *Information systems supporting services are hosted on a dedicated internal network. Radiomics members participating in te project can access this network from the building or remotely by using a VPN connection.* *Preventing data loss* *Low probability and high impact as data received are backed up and accessible in read-only to avoid deletion/modification.*
12. Identification and incident response plan in case of a data breach (incl. 3th parties)		
12.1	Preventive measures	*Radiomics strongly believes in preventive measures to avoid incidents, rather than solving incidents. As such, the impact of a potential data breach is calculated for every data point in the company, using a methodology derived from the ENISA framework. This risk score is kept in the data register next to the respective data point. Our risk prevention and monitoring efforts are prioritized in line with the calculation (highest risk = highest level of attention & security measures)*
12.2	Description of the incident response plan (upon a data breach) & logging	*Radiomics has setup a security event management with supporting ticketing and reaction system. Depending on the severity of the risk, the notifications and involved people are defined and relevant actions are triggered. This is defined in specific procedures in our QMS (P-DAT-06 Personal Data Breach).* *Radiomics is continuously working to extend the range of automatic monitoring for abnormalities. E.g.: On-premises servers are monitored by a solution automatically monitoring the status of servers and running processes.*
13. Data localisation, exchange and integration (EU/non-EU countries)		
13.1	Indicate which countries (within the EU) and which parties are involved (in terms of storage/exchange/processing/integration).	*Belgium, Italy, Poland, Ireland and Portugal*
13.2	Countries / parties involved outside of the EU (in terms of storage/exchange/ processing/integration)	*Two actors involved in the study have their main establishment in third countries, namely AstraZeneca and Google.* *The Global Headquarters of AstraZeneca are located in the UK (1 Francis Crick Avenue, Cambridge Biomedical Campus, Cambridge CB2 0AA). The UK benefits from an Adequacy Decision of the European Commission, which means that personal data can be freely transferred to the UK , as is the case within the European Economic Area (hereinafter: EEA). Furthermore, in the DTA, AstraZeneca undertakes not to transfer personal data outside the EEA and the UK.* *The Global Headquarters of Google are located in the US (1600 Amphitheatre Parkway Mountain View, Googleplex, CA 94043). Since July 2023, the US benefit from an Adequacy Decision of the European Commission, called the Data Privacy Framework. This means that personal data can be freely transferred to US entities that participate in the Data Privacy Framework, which is the case with Google. In the context of the study, GCP services will be used to store imaging and clinical data during transfer, on a server based in the EEA (Belgium). Furthermore, any imaging and clinical data going through Google's infrastructure will be encrypted to ensure data content cannot be read by Google.*
13.2.1	Measures to enforce GDPR outside of EU	*No data outside EU is expected to be collected for this project. The two countries, where actors involved in this study are established (the US and the UK), benefit from an adequacy decision.*
13.2.2	Safe list or adequacy agreement?	*N/A*
14.Profiling (processing of data for marketing or commercial purposes (incl. automated decision making/marketing automation)?		
14.1	Is the personal data in scope of this initiative used for commercial or marketing means?	*No*
14.1.1	Will the personal data be used for commercial/marketing purposes? If so, is there a legal basis?	*N/A*
14.1.3	Can we make sure that customers/data subjects which have refused either certain channels of communication, profiling or commercial/marketing activities will not be contacted for commercial means (and that their personal data is not processed accordingly (commercial/marketing means)).	*N/A*
14.1.4	Are any specific lists/registers used when approaching customers for commercial/marketing means?	*N/A*
15. Use of cookies or any other techniques (e-privacy directive)?		
15.1	Are cookies or any other similar tools (web beacons, app fingerprinting, tracking,...) used?	*No*
16. Reporting of processing or DPIA itself to be provided to the DPA?		
16.1	Should the processing/storage included in this initiative (or outcome of this DPIA) be notified to the DPA?	*No*
17. Controller vs. Processor		
17.1	Have controller (joint controller) & processors been identified in all personal data flows?	*AstraZeneca is the sponsor of the study and has decided the analysis we will be performed by Radiomics. For that reason AstraZeneca is the controller and Radiomics.bio is the processor of the data. The participating will act as seperate data controllers (from each other and from AstraZeneca). The sites will be and will remain the owner of the data.*
17.2	Are all agreements with controllers, processors & co-controllers compliant?	*Yes*
18. Other risks		
18,1	Are there any other privacy or data protection risks which have not been mentioned or sufficiently explained in this DPIA	*Human error is a potential risk that can, for example, lead to the accidental sharing of patient information when it is not correctly pseudonymised.* *To minimize this, newcomers will receive comprehensive onboarding training. At Radiomics any team member can need training at any moment in their career. This need is triggered by onboarding, a change in job description, a new or updated process or tool used in the company, a spontaneous request of the team member, ... (non-exhaustive list). This need can also be identified during a performance evaluation, which are conducted twice a year.* *Details on staff training can be found at P-HUM-01 Staff Management.*
18,2	Have any other (not indicated yet) risks been evaluated with regards to the rights and freedoms of natural persons?	*No*
19. Technical questions		
19.1	Have the systems, processes and org taken into account the principles of data protection by design and by default?	*Yes, Radiomics' infrastructure is composed of two main parts. A data transfer platform (Share server), and the main computing environment. These two parts are physically and logically disconnected. Any incoming data will be transferred to Radiomics' systems through the Share server. Before being forwarded to the main computing environment, this data will be checked for proper de-identification by the relevant personnel. Access to the Share server follows the least privilege principle, and data do not stay on this server after transfert completion. Personnel ensuring the proper data deindentification is distinct from the personnel subsequently processing the data.*
19.2	Describe the processes and solutions which provide a solution for storing and managing consent and/or legal ground	*Data is collected as per GDPR and local lab. Consent will not be collected from the patients, therefore consent management is NAP.*
20. Code of conducts and other legal agreements		
20.1	Have any other legal frameworks been agreed upon between the parties involved?	*No*
20.2	How do the additional frameworks exceed or deviate from GDPR?	*N/A*
21. Conclusion and signature of the DPO		
21.1	Opinion of the DPO	After analysing the risks and risk mitigation measures, taking into account the fundamental rights and freedoms of the data subjects and balancing the interests of all concerned, it appears that, if the mitigation measures are put in place to protect the personal data of the data subjects, there is no high residual risk that could lead to high-risk negative consequences for data subjects. Consequently, the DPO approves the waiver of the collection of data subjects' consent for the study, given the context described in the DPIA and the mitigating measures.
21.2	Signature of the DPO	Data Protection Officer, Helena Peten de Pina Prata Zaventem, 11/10/2024