Data Processing Agreement

Case study title: DPA (Data Processing Agreement)

Description

The General Data Protection Regulation (GDPR) regulates the processing of personal data in Europe through data processing agreements (DPAs). The GDPR imposes obligations onto organizations as long as they collect, process, or handle in any way the personal data of people in Europe. Thus, organizations that have software systems that involve processing or sharing personal data are responsible for conducting audits to ensure their data processing satisfies GDPR obligations. To achieve software compliance, organizations must verify their software-relevant legal documents against GDPR regulations. Organizations do this through DPAs that regulate data processing activities according to GDPR. These are legally binding agreements and to be deemed GDPR-compliant, DPAs must cover all criteria imposed by GDPR provisions concerning data processing.

Data processing involves an organization, known as the data controller, which collects and/or further shares personal data, an additional organization, known as the data processor, which processes personal data for the controller, and of course a data subject who shares personal data willingly. A third-party organization, called a sub-processor, may be employed by the data processor to perform some data processing services on its behalf. This involves further sharing the personal data. The controller provides data subjects with the terms on which their personal data is collected and handled. However, further sharing of personal data with processors and sub-processors is not directly visible to data subjects. The controller and processor share responsibility of protecting personal data. Thus, a DPA listing privacy-related requirements should be established between controller and processor(s). A DPA includes setting terms for how data is used, stored, protected, and accessed. Establishing a DPA also includes the rights and obligations of the controller and processor. Signing a DPA means that the processor is obliged to ensure that any software system deployed for processing personal data has to also comply with GDPR.

The paper which this case study is drawn from uses the “shall” requirements that the authors extracted from GDPR provisions relevant to DPA compliance, which removes the additional complexity and potential ambiguity of legal texts. DPAs are an important source of requirements for software development involving the processing of personal data. SLEEC requirements allow the controller and processor to be legally-compliant with the GDPR. For instance, we can specify that upon the end of the provision of services relating to processing, the processor shall

return or delete all personal data, or that the DPA shall contain the duration of the processing, after which data return/removal occurs.

Stage of Development (Technical contributor)

Existing Regulation

Expert info
Expertise of the stakeholders involved in devising the SLEEC rules
Number of stakeholders writing the rules

Stakeholder names	Expertise
TS-1	Engineer/Goal Modelling
N-TS-1	Ethics

1. **Normative requirements**

    a. **Normative requirements in natural language**

    Normative requirements in natural language, in blue the corrected requirements after using N-Tool.

A = autonomy, *PH = psychological health (non-maleficence)*, P = privacy, E = explainability, T = transparency, CS = cultural sensitivity, SR = social requirement, B 'beneficence' (doing good), N 'non-maleficence' (preventing/avoiding harm), and S 'safety'. "+" and "-" for positive and negative impacts respectively.

rule id	rule	impact	label(s) (social, legal, ethical, empathetic, or cultural)	stakeholder expertise	authors identifiers
1	When DPA is made, the DPA shall contain a controller's identity and contact details - If not, the DPA shall be incomplete	+T +E +S	Legal	Engineer/Goal Modelling	TS-1

2	When DPA is made, the DPA shall contain a processor's identity and contact details - If not, the DPA shall be incomplete	+T +E +S	Legal	Engineer/Goal Modelling	TS-1
3	When DPA is made, the DPA shall contain the duration of the processing.	+T +E +S	Legal	Engineer/Goal Modelling	TS-1
4	When DPA is made, the DPA shall contain the nature and purpose of the processing. - If not, the DPA shall be incomplete	+T +E +S	Legal	Engineer/Goal Modelling	TS-1
5	When DPA is made, the DPA shall contain the types of personal data. - If not, the DPA shall be incomplete	+T +E +S	Legal	Engineer/Goal Modelling	TS-1
6	When DPA is made, the DPA shall contain the categories of data subjects. - If not, the DPA shall be incomplete	+T +E +S	Legal	Engineer/Goal Modelling	TS-1
7	~~The processor shall not engage a sub-processor~~ ~~• Unless prior specific or general written authorization from controller is obtained~~ The processor shall not engage a sub-processor without prior specific or general written authorization from controller	+P +T +E +S	Legal	Engineer/Goal Modelling	TS-1

	• When there is no general or specific written authorization, the processor must contact controller and obtain consent				
8	When there is general written authorization from the controller and there are changes concerning the addition or replacement of sub-processors, the processor shall inform the controller of any intended changes	+P +T +E	Legal, Social	Ethics, Engineer/Goal Modelling	N-TS-1, TS-1
9	The processor shall not process personal data • Unless there are documented instructions from the controller	+P +T +E +S	Legal	Ethics	N-TS-1
10	If the processor requires by Union or Member State law to process personal data without instructions, the processor shall inform the controller of that legal requirement before processing • Unless the law prohibits informing the controller	+P +T +E +SR	Legal, Social, Cultural	Ethics	N-TS-1
11	The processor shall ensure that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality	+P +T +E +S +N +SR	Legal, Ethical, Social, Empathetic	Engineer/Goal Modelling	TS-1

12	The processor shall take all measures required pursuant to Article 32 or to ensure the security of processing	+P +T +E +S +N	Legal, Ethical	Engineer/Goal Modelling	TS-1
13	The processor shall assist the controller in fulfilling its obligation to respond to requests for exercising the data subject's rights - When responding to requests, the processor shall inform the data subject	+P +T +E +SR	Legal, Ethical	Engineer/Goal Modelling	TS-1
14	The processor shall assist the controller in ensuring the security of processing	+P +T +E +S +N	Legal, Ethical	Engineer/Goal Modelling, Ethics	TS-1, N-TS-1
15	The processor shall assist the controller in notifying a personal data breach to the supervisory authority	+E +T	Legal	Engineer/Goal Modelling	TS-1
16	The processor shall assist the controller in communicating a personal data breach to the data subject	+T +E -PH -P -N	Legal, Ethical, Empathetic	Engineer/Goal Modelling, Ethics	TS-1, N-TS-1
17	The processor shall assist the controller in ensuring compliance with the obligations pursuant to data protection impact assessment	+P +T +E +N	Legal	Engineer/Goal Modelling	TS-1

18	If processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, then prior to processing, the processor shall assist the controller in consulting the supervisory authorities	+T +E +N +S	Legal, Ethical	Ethics, Engineer/Goal Modelling	N-TS-1, TS-1
19	The processor shall return or delete all personal data to the controller after the end of the provision of services relating to processing	+T +E +P	Legal, Ethical	Engineer/Goal Modelling	TS-1
20	The processor shall immediately inform the controller if an instruction infringes the GDPR or other data protection provisions	+T +E -P	Legal, Ethical	Engineer/Goal Modelling	TS-1
21	The processor shall make available to the controller information necessary to demonstrate compliance with the obligations Article 28 in GDPR	+T +E +N +P	Legal	Engineer/Goal Modelling	TS-1
22	The processor shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller	+T +E +N	Legal, Ethical, Empathetic	Engineer/Goal Modelling	TS-1
23	The processor shall impose the same obligations on the engaged sub-processors by way of contract or other legal act under Union or Member State law	+SR +T +E	Legal, Cultural, Social	Engineer/Goal Modelling	TS-1
24	The processor shall	+S	Legal	Engineer/Goal	TS-1

	remain fully liable to the controller for the performance of sub-processor's obligations	+E		Modelling	
25	~~The processor shall assess the level of security and take into account the risk of accidental or unlawful destruction, loss, alternation, unauthorized disclosure of or access to the personal data transmitted, stored or processed~~ The processor shall evaluate (i.e pass or not pass) the level of security and take into account the risk of accidental or unlawful destruction, loss, alternation, unauthorized disclosure of or access to the personal data transmitted, stored or processed. - If the level of security does not pass evaluation, then the processor will inform the controller	+N +S +P	Legal, Ethical, Empathetic	Engineer/Goal Modelling	TS-1
26	When the processor has informed the controller of changes concerning the addition or replacement of sub-processors, and when there has been general written authorization, the controller shall approve the changes ● Unless the controller wishes to	+T +E +A	Legal	Engineer/Goal Modelling, Ethics	TS-1, N-TS-1

	object to changes				

Concerns	
c1	When the DPA is made and all the necessary components for it to be complete are there, it is not marked complete
c2	The data processor (and/or sub-processors) keeps personal data after processing has been complete
c3	The data processor (and/or sub-processors) did not ensure security of data prior to processing
c4	The controller shares personal data to an organization that is not an approved data processor
c5	The processor did not respond to requests for exercising the data subject's rights
c6	The processor processed personal data even when processing would result in a high risk of a data breach
c7	The processor does not inform the controller if an instruction infringes the GDPR or other data protection provisions.
c8	The data subject is not informed of a data breach
c9	Passes security when evaluated, even if there is risk
c10	Does not inform controller of changing (add/remove) subprocessor
c11	Does not allow audits even when there is an audit and auditor
Purpose	
p1	The supervisor must be informed in the case of a data breach
p2	The data subject must be informed in the case of a data breach
p3	When a data subject requests their rights, the processors and sub-processors must assist the controller
p4	When there are changes to the DPA being made, the processor must obtain controller consent
p5	The DPA process must be able to process after it has been started and there is data to process, controller instructions have been given, and confidentiality and security has been ensured.
p6	The processor must be able to inform control while processing personal data and confidentiality and security has been ensured.
p7	The DPA must be able to pass security after being evaluated
p8	The processor must be able to inform the controller when the law requires it and informing is

	allowed
99	The DPA process must be able to start once there are controller instructions and the rules do not conform yet
p10	The DPA must be able to terminate if it is incomplete
p11	The DPA must be able to be complete if it has been made
Impact keys: A = autonomy, PH = psychological health (non-maleficence), P = privacy, E = explainability, T = transparency, CS = cultural sensitivity, SR = social requirement, B 'beneficence' (doing good), N 'non-maleficence' (preventing/avoiding harm), and S 'safety'. "+" and "-" for positive and negative impacts respectively.	

1. **Rules in the SLEEC DSL**

The stakeholders corrections after analyzing the well-formedness of the rules using our N-Tool are commented and in blue.

```
def_start
        event DPAMade
        // For DPA shall contain (i.e regarding completion)
        // DPA initial terms
        event EvaluateDPAProcess            // Prior to starting processing
        event StartDPAProcess               // Process information started
        event DPAComplete
        event DPAIncomplete
        // After DPA completion, events that can happen
        event DPATerminate                  // If DPA agreement has expired
        event DPAUpdate                     // Making changes to agreement (after DPAComplete)
        event ProcessPersonalData
        event RemovePersonalData
        // Events processor is doing for controller
        event EngageSubProcessor
        event ChangeSubProcessor
        event InformController          // Concerning the addition or replacement of sub-processors
        event AssistController
        event ProvideControllerInformation
        event ObtainControllerConsent       // Obtain controller authorization

        event InformSubject
        event InformSupervisor
        event TakeLiabilityForSubProcessor
        event ImposeObligationsOnSubProcessor
        // Events that happen to DPA
        event DataBreach
        event RightsRequested
```

```
        event RespondToRequest
        event AllowAudits
        event HelpAuditors
        event AuditsOccur //created
        event EvaluateSecurity //created
        event PassSecurity //created
        event CanObjectToChange //created
        // event DPACompliant //created

        measure controllerID: boolean
        measure controllerInfo: boolean
        measure processorID: boolean
        measure processorInfo: boolean
        measure dpaPurpose: boolean
        measure dpaNature: boolean
        measure dpaCategories: boolean
        measure dpaLength: numeric                  // Length of DPA processing, i.e years
        measure dpaActive: boolean                  // Whether or not the DPA agreement is active
        measure dataCompliance: boolean
        measure specificControllerAuth: boolean     // Specific controller authorization
        measure genControllerAuth: boolean          // General controller authorization
        measure controllerInstructions: boolean     // Controller gave processor instructor or not
        measure rulesConform: boolean               // If goes along with GDPR rules
        measure personalData: boolean               // Whether or not personal data exists
        measure lawRequires: boolean                // Law requires processing without controller
        measure informingAllowed: boolean           // Processor allowed to inform Controller
        measure confidentialityEnsured: boolean     // Agreed to be confidential about personal data
        measure securityEnsured: boolean            // Security about personal data ensured
        measure measureTaken: boolean               //TODO: to make it concrete
        measure riskLevel: scale(low, medium, high)
        measure typesOfRisk: scale(dataDestruction, dataLoss, dataAlter, unauthDataAccess)
        measure auditorType: scale(controller, mandatedAuditor)
        measure auditType: scale(audit, inspection)
        measure art28Compliance: boolean
def_end
rule_start
        // Measures that need to be true (things DPA needs to contain) in order to be complete
        // 1. The DPA shall contain at least one controller's identity and contact details
        // 2. The DPA shall contain at least one processor's identity and contact details
        // 4. The DPA shall contain the nature and purpose of the processing
        // 5. The DPA shall contain the types of personal data
        // 6. The DPA shall contain the categories of data subjects
        r1 when DPAMade then DPAComplete
                unless (((((((not {controllerID}) or (not {controllerInfo})) or (not {processorInfo}))
                or (not {processorID})) or (not {dpaPurpose})) or (not {dpaNature})) or (not
                {dpaCategories})) then DPAIncomplete
        //*************************************************************************
        // Resolve concern 1 (Refine R1)
        // Comment R1, and uncomment R1
```

```
        //R1 when DPAMade then DPAComplete
            // unless (((((((not {controllerID}) or (not {controllerInfo})) or (not {processorInfo}))
            // or (not {processorID})) or (not {dpaPurpose})) or (not {dpaNature})) or (not
{dpaCategories})) then not DPAIncomplete
        //*********************************************************************

        // 3. The DPA shall contain the duration of the processing
        r2 when DPAMade and (({dpaLength} > 0) or {dpaActive}) then DPAComplete
                otherwise DPATerminate
        // 7. The processor shall not engage a sub-processor without a prior specific or general written
        authorization of the controller
        r3 when DPAUpdate then EngageSubProcessor
                unless ((not {specificControllerAuth}) or (not {genControllerAuth})) then
ObtainControllerConsent
        //*********************************************************************
        //** Resolve concern c4 (ADD two rules, R3_0 and R3_1)
        // Uncomment R3_0,  R3_1 and comment R3
        // R3_0 when DPAUpdate and ((not {specificControllerAuth}) or (not {genControllerAuth})) then
not EngageSubProcessor
        // R3_1 when DPAUpdate and ((not {specificControllerAuth}) or (not {genControllerAuth})) then
ObtainControllerConsent
        //*********************************************************************
        // 8. In case of general written authorization, the processor shall inform the controller of any
        intended changes concerning the addition or replacement of sub-processors
        R4 when ChangeSubProcessor and {genControllerAuth} then InformController
        // 9. The processor shall process personal data only on documented instructions from the
        controller
        // 10. If the processor requires by Union or Member State law to process personal data without
        instructions and law does not prohibit informing the controller on grounds of public interest, the
        processor shall inform the controller of that legal requirement BEFORE processing
        // 11. The processor shall ensure that persons authorized to process personal data have
        committed themselves to confidentiality or are under an appropriate statutory obligation of
        confidentiality
        // 12. The processor shall take all measures required pursuant to Article 32 or to ensure the
        security of processing
        R5 when StartDPAProcess and ((({controllerInstructions} and {personalData}) and
        {confidentialityEnsured}) and {securityEnsured}) then ProcessPersonalData
            unless ({lawRequires} and {informingAllowed}) then InformController
        // When there is personalData to process, and you have informed controller, you can process
        R6 when InformController and (({personalData} and {confidentialityEnsured}) and
        {securityEnsured}) then ProcessPersonalData
        // 13. The processor shall assist the controller in fulfilling its obligation to respond to requests for
        exercising the data subject's rights
        // As a processor
        R7 when RightsRequested then AssistController
        // As a controller
        R8 when RightsRequested then RespondToRequest
        //*********************************************************************
        //** Resolve concern c5 (ADD a rule, R8_0)
```

```
// R8_0 when RespondToRequest then InformSubject
//*************************************************************************
// 14. The processor shall assist the controller in ensuring the security of processing
// 17. The processor shall assist the controller in ensuring compliance with the obligations pursuant to data protection impact assessment
R9 when StartDPAProcess and ((not {securityEnsured}) or (not {dataCompliance}))
then AssistController
// 15. The processor shall assist the controller in notifying a personal data breach to the supervisory authority
// 16. The processor shall assist the controller in communicating a personal data breach to the data subject
R10 when DataBreach then InformSupervisor
R11 when DataBreach then InformSubject
// 18. The processor shall assist the controller in consulting the supervisory authorities prior to processing where the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk
R12 when EvaluateDPAProcess and ((not {measureTaken}) and ({riskLevel} = high))
then not StartDPAProcess
R13 when EvaluateDPAProcess and ((not {measureTaken}) and ({riskLevel} = high))
then InformSupervisor
// 19. The processor shall return or delete all personal data to the controller after the end of the provision of services relating to processing
R14 when StartDPAProcess and (({dpaLength} <= 0) or (not {dpaActive}))
then RemovePersonalData
// 20. The processor shall immediately inform the controller if an instruction infringes the GDPR or other data protection provisions
R15 when StartDPAProcess and ({controllerInstructions} and (not {rulesConform}))
then InformController
// 21. The processor shall make available to the controller information necessary to demonstrate compliance with the obligations Article 28 in GDPR
R16 when StartDPAProcess and (not {art28Compliance}) then ProvideControllerInformation
// 22. The processor shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller
R17 when AuditsOccur and (((({auditType} = audit) or ({auditType} = inspection)) or
({auditorType} = controller)) or ({auditorType} = mandatedAuditor)) then AllowAudits
R18 when AuditsOccur and (((({auditType} = audit) or ({auditType} = inspection)) or
({auditorType} = controller)) or ({auditorType} = mandatedAuditor)) then HelpAuditors
// 23. The processor shall impose the same obligations on the engaged sub-processors by way of contract or other legal act under Union or Member State law
R19 when EngageSubProcessor then ImposeObligationsOnSubProcessor
// come back to this and add legal act?
// 24. The processor shall remain fully liable to the controller for the performance of sub-processor's obligations
R20 when EngageSubProcessor then TakeLiabilityForSubProcessor
// 25. When assessing the level of security, the processor shall take into account the risk of accidental or unlawful destruction, loss, alternation, unauthorized disclosure of or access to the personal data transmitted, stored or processed
R21 when EvaluateSecurity then PassSecurity
unless ({personalData} and ((((({typesOfRisk} = dataDestruction) or ({typesOfRisk} =  dataLoss))
```

```
        or ({typesOfRisk} = dataAlter)) or ({typesOfRisk} = unauthDataAccess) ) and ({riskLevel} > low)))
        then InformController

        //*************************************************************************
        //** Resolve concern c9 (ADD two rules,  R21_0 and R21_1)
        // address c9 (replace R21 rule by two rules R21_0, r21_1(ADD and DELETE))
        // r21_0 when EvaluateSecurity and ({personalData} and ((((({typesOfRisk} = dataDestruction) or
({typesOfRisk} =  dataLoss)) or ({typesOfRisk} = dataAlter)) or ({typesOfRisk} = unauthDataAccess) ) and
({riskLevel} > low))) then not PassSecurity

        //r21_1 when EvaluateSecurity and ({personalData} and ((((({typesOfRisk} = dataDestruction) or
({typesOfRisk} =  dataLoss)) or ({typesOfRisk} = dataAlter)) or ({typesOfRisk} = unauthDataAccess) ) and
({riskLevel} > low))) then InformController
        //*************************************************************************
        // 26. In case of general written authorization, the controller shall have the right to object to
        changes concerning the addition or replacement of sub-processors, after having been informed of
        such intended changes by the processor
        r22 when InformController and {genControllerAuth} then CanObjectToChange
rule_end

concern_start
        // The DPA is never completed
        c1 when DPAMade and ({controllerID} and ({controllerInfo} and ({processorInfo} and
        ({processorID} and ({dpaPurpose} and ({dpaNature} and {dpaCategories})))))) then not
        DPAComplete
        // The data processor (and/or sub-processors) keeps personal data after processing has been
        complete
        c2 when StartDPAProcess and (({dpaLength} <= 0) or (not {dpaActive}))
                then not RemovePersonalData
        // The data processor (and/or sub-processors) did not ensure security of data prior to processing
        c3 when StartDPAProcess and ({controllerInstructions} and ({personalData} and
({confidentialityEnsured} and ({securityEnsured} and ((not {lawRequires}) and (not
{informingAllowed}))))))) then not ProcessPersonalData
        // The controller shares personal data to an organization that is not an approved data processor
        c4 when DPAUpdate and ((not {specificControllerAuth}) or (not {genControllerAuth})) then
EngageSubProcessor
        // The processor did not respond to requests for exercising the data subject's rights
        c5 when RightsRequested then not InformSubject
        // The processor processed personal data even when processing would result in a high risk of a
        data breach
        c6 when EvaluateDPAProcess and ((not {measureTaken}) and ({riskLevel} = high)) then
StartDPAProcess
         // The processor does not inform the controller if an instruction infringes the GDPR or other data
        protection provisions.
        c7 when StartDPAProcess and ({controllerInstructions} and (not {rulesConform}))
        then not InformController
         // Does not inform subject of databreach
        c8 when DataBreach then not InformSubject
        // Passes security when evaluated, even if there is risk
```

c9 **when** EvaluateSecurity **and** ({personalData} **and** ((((({typesOfRisk} = dataDestruction) **or** ({typesOfRisk} = dataLoss)) **or** ({typesOfRisk} = dataAlter)) **or** ({typesOfRisk} = unauthDataAccess)) **and** ({riskLevel} > low))) **then** PassSecurity

// Does not inform controller of changing (add/remove) subprocessor

c10 **when** ChangeSubProcessor **and** {genControllerAuth} **then not** InformController

// Does not allow audits even when there is an audit and auditor

c11 **when** AuditsOccur **and** (((({auditType} = audit) **or** ({auditType} = inspection)) **or** ({auditorType} = controller)) **or** ({auditorType} = mandatedAuditor)) **then not** AllowAudits

concern_end

purpose_start

pr1 **exists** DPAMade
pr2 **exists** EvaluateDPAProcess
pr3 **exists** StartDPAProcess
pr4 **exists** DPAComplete
pr5 **exists** DPAIncomplete
pr6 **exists** DPATerminate
pr7 **exists** DPAUpdate
pr8 **exists** ProcessPersonalData
pr9 **exists** RemovePersonalData
pr10 **exists** EngageSubProcessor
pr11 **exists** ChangeSubProcessor
pr12 **exists** InformController
pr13 **exists** AssistController
pr14 **exists** ProvideControllerInformation
pr15 **exists** ObtainControllerConsent
pr16 **exists** InformSubject
pr17 **exists** InformSupervisor
pr18 **exists** TakeLiabilityForSubProcessor
pr19 **exists** ImposeObligationsOnSubProcessor
pr20 **exists** DataBreach
pr21 **exists** RightsRequested
pr22 **exists** RespondToRequest
pr23 **exists** AllowAudits
pr24 **exists** HelpAuditors
pr25 **exists** AuditsOccur //created
pr26 **exists** EvaluateSecurity //created
pr27 **exists** PassSecurity //created
pr28 **exists** CanObjectToChange //created

// The purpose of the data subject is to preserve user privacy

P1 **exists** InformSupervisor **while** DataBreach
P2 **exists** InformSubject **while** DataBreach
P3 **exists** AssistController **while** RightsRequested
P4 **exists** ObtainControllerConsent **while** DPAUpdate

// The purpose of the data processor is to process personal data

P5 **exists** ProcessPersonalData **and** ((({controllerInstructions} **and** {personalData}) **and** {confidentialityEnsured}) **and** {securityEnsured}) **while** StartDPAProcess

```
        P6 exists ProcessPersonalData and (({personalData} and {confidentialityEnsured}) and
{securityEnsured}) while InformController
        // A completed DPA must explicitly cover all GDPR provisions concerning data processing
        P7 exists PassSecurity while EvaluateSecurity
        P8 exists InformController and ({lawRequires} and {informingAllowed})
        P9 exists StartDPAProcess and ({controllerInstructions} and (not {rulesConform}))
        // The purpose of the DPA is to be complete
        P10 exists DPATerminate while DPAIncomplete
        P11 exists DPAComplete while DPAMade
purpose_end
```