

Notisums allmänna villkor för nät-tjänster

Gällande fr.o.m. 2023-12-01 och tills vidare.

1. Allmänt

1.1. Dessa allmänna villkor gäller för den eller de Internettjänster, konsultprodukter och liknande tjänster och produkter som vid var tid tillhandahålls av Notisum AB, org.nr. 556516–2467, ("**Notisum**").

1.2. Notisum uppdaterar fortlöpande sitt utbud av tjänster och produkter och förbehåller sig rätten att ändra, ta bort eller lägga till information i erbjudna tjänster och produkter, samt upphöra att tillhandahålla dessa.

1.3. Avtal om tillgång till tjänster och produkter som tillhandahålls av Notisum ingås av ett bolag eller annan juridisk person ("**Licenstagaren**") för dess anställdas [och uppdragstagares] ("**Användarna**") användning av tjänsterna och produkterna. Samtliga Användare ska vid första inloggning i Tjänsterna (definierat nedan) godkänna dessa allmänna villkor.

1.4. Abonnemangsavtal mellan Notisum och Licenstagaren ("**Abonnemangsavtalet**") omfattar de tjänster och produkter som vid var tid omfattas av Abonnemangsavtalet ("**Tjänsterna**"), och tillhandahålls på de ekonomiska villkor som parterna kommit överens om i Abonnemangsavtalet, samt i enlighet med dessa allmänna villkor.

1.5. Licenstagaren får inte upplåta eller överlåta sina rättigheter enligt Abonnemangsavtalet till tredje man utan Notisums i förväg lämnade skriftliga tillstånd. Vid eventuell överlåtelse ska ny avtalspart skriftligen bekräfta att denne godtar bestämmelserna i Abonnemangsavtalet och dessa allmänna villkor.

2. Upplåtelse och rättigheter

2.1. Samtliga rättigheter till Tjänsterna och dess innehåll, inklusive upphovsrätt och alla andra immateriella rättigheter, tillhör Notisum och/eller tredje part med vilken Notisum träffat avtal. Uppgifter om upphovsrätt/copyright och andra äganderättsmeddelanden i Tjänsterna eller på levererad produkt och därtill hörande dokumentation ska bibehållas av Licenstagaren och får inte avlägsnas eller göras oläslig.

2.2. Licenstagaren och Användarna erhåller inte någon rätt till Tjänsterna utöver vad som uttryckligen anges i Abonnemangsavtalet och dessa allmänna villkor.

2.3. Notisum upplåter till Licenstagaren en icke exklusiv, icke upplåtbar eller överlåtbar, rätt att under Abonnemangsavtalets giltighetstid låta Användarna använda Tjänsterna i enlighet med Abonnemangsavtalet och dessa allmänna villkor, och i samband därmed kopiera, bearbeta eller framställa sammanställningar av innehållet i Tjänsterna, såsom laglistor och andra liknande arbetsprodukter som helt eller delvis är baserade på Tjänsterna ("**Resultat**"), allt för Licenstagarens interna bruk och i enlighet med Abonnemangsavtalet och dessa allmänna villkor.

2.4. Med "**Licenstagarens interna bruk**" menas användning av Tjänsterna och Resultatet för Licenstagarens egen verksamhet, men inte att Licenstagaren vidareupplåter eller vidareförmedlar Tjänsterna till tredje man. Närmare om gränserna mellan tillåten och otillåten användning av Tjänsterna och Resultatet anges nedan.

3. Närmare om användning av Tjänsterna

3.1. Tjänsterna får endast användas av Användarna för det syfte som de är framtagna och endast för lagliga ändamål. Användarna får inte upplåta eller överlåta sin rätt till användning av Tjänsterna eller delar därav eller på annat sätt disponera eller förfoga över Tjänsterna. Om en Användare upphör att vara anställd eller uppdragstagare hos Licenstagaren upphör dennes rätt att använda Tjänsterna i samband därmed.

3.2. Användarna ansvarar för att förvara lösenord eller andra användarbehörigheter på ett säkert sätt. Användarna kan begära att Notisum spärrar Tjänsterna eller att Notisum tillhandahåller Användaren ett nytt lösenord.

3.3. Användarna får inte, utöver vad som krävs för Användarnas egen användning av Tjänsten, överlåta, upplåta eller på annat sätt sprida lösenord eller andra användarbehörigheter som de tilldelats av Notisum.

3.4. Vid användningen av Tjänsterna är Användarna även skyldiga att iaktta övriga föreskrifter, anvisningar och begränsningar för respektive Tjänst samt övriga anvisningar som utfärdas av Notisum eller tredje part med vilken Notisum träffat avtal.

3.5. Notisum har rätt att utan föregående varning stänga av Användare från vidare användning av Tjänsterna om misstanke finns om att denne använder Tjänsterna i strid med dessa allmänna villkor.

3.6. Användarna kan inom ramen för Tjänsterna och enligt de närmare begränsningar som meddelas av Notisum lagra Resultat samt av Användaren uppladdade dokument hos Notisum. Licenstagaren ansvarar för att all sådan lagring och behandling av materialet sker i enlighet med vid var tid gällande lagstiftning. Notisum ska behandla sådant material konfidentiellt. Licenstagaren ska hålla Notisum skadeslöst för alla ersättningskrav, kostnader och andra eventuella skador som sådant material kan orsaka Notisum. Notisum förbehåller sig rätten att radera sådant material vid misstanke om att det inte lagrats och/eller behandlats i enlighet med gällande lagstiftning och om Användarnas rätt att använda Tjänsterna upphör. Användaren är ansvarig för att säkerhetskopiera Resultatet och av Användaren uppladdade dokument.

4. Testperiod

4.1. Om Notisum och Licenstagaren träffat särskild överenskommelse om en testperiod avseende Tjänsterna, gäller följande.

4.2. Överenskomna och namngivna Användare får under den begränsade tid som anges i överenskommelsen ("**Testperioden**") tillgång till Tjänsterna i syfte att testa dessa. Ingen ersättning utgår till Notisum för sådan användning av Tjänsterna.

4.3. Vid all användning av Tjänsterna under Testperioden gäller dessa allmänna villkor i tillämpliga delar med undantag för betalningsbestämmelsen, punkt 9.

5. Behandling av personuppgifter

5.1. Notisum är personuppgiftsansvarig för de personuppgifter som lämnas av Licenstagaren och/eller Användarna i samband med beställning och/eller användning av Tjänsterna. Närmare information om hur Notisum behandlar personuppgifter finns i [Notisums integritetspolicy](#).

5.2 För det fall Notisum och Licenstagaren har överenskommit att personuppgifter får lagras i Tjänsterna kommer Notisum enligt Dataskyddsförordningen att ha en roll som personuppgiftsbiträde i förhållande till Licenstagaren som personuppgiftsansvarig. I sådana fall gäller Annex 1, Data Processing Agreement (Personuppgiftsbiträdesavtal), i den utsträckning Notisum behandlar personuppgifter för Licenstagarens räkning.

6. Tekniska krav

6.1. Se Notisums hemsida [www.notisum.se] för vid var tid gällande tekniska krav som måste vara uppfyllda för att Användarna ska få tillgång till Tjänsterna och Tjänsternas rätta funktion.

6.2. Licenstagaren och Användaren ansvarar för att de tekniska kraven är uppfyllda samt att det finns en fungerande uppkoppling mellan Användaren och Anslutningspunkten (se definition nedan). Vidare ansvarar Licenstagaren och Användaren för de därmed förenade kostnaderna samt för installation av all eventuell erforderlig programvara.

7. Leverans och support

7.1. Tjänsterna tillhandahålls i av Notisum anvisad anslutningspunkt ("**Anslutningspunkten**"). Om inteparterna har kommit överens om annat är Anslutningspunkten den punkt eller punkterna som Notisum kopplar samman Tjänsterna med Internet.

7.2. Se Notisums hemsida [www.notisum.se] för Tjänsternas öppettider m.m. Under avtalstiden har Notisum rätt att helt eller delvis stänga ned en eller flera Tjänster för att utföra uppdatering, underhåll och liknande åtgärder (se Notisums hemsida [www.notisum.se] för närmare information om planerade underhållsåtgärder).

7.3. Teknisk support och användarsupport, (tillsammans "**Support**") för Tjänsterna, tillhandahålls av Notisum, eller av tredje man för Notisums räkning, på vardagar och under kontorstid (se Notisums hemsida [www.notisum.se] för den lokala supportens kontaktuppgifter och öppettider m.m.). Till dess annat anges av Notisum tillhandahålls Support utan särskild ersättning.

7.4. Support innefattar inte support, underhåll, felsökning/felavhjälpning eller liknade åtgärder avseende Licenstagarnas eller Användarnas program- eller maskinvara, internetförbindelser och/eller produkter/tjänster som inte tillhandahållits av Notisum eller för vilka inte Notisum uttryckligen ansvarar. Support innefattar inte heller frågor kring tillämpningen av den lagstiftning och andra regelverk som omfattas av leveransen av Tjänsterna.

8. Fel eller brister

8.1. Vid fel eller brist i Tjänsterna i Anslutningspunkten, ska Licenstagaren kontakta Notisum för åtgärd (se Notisums hemsida [www.notisum.se] för kontaktuppgifter för felanmälan).

8.2. Notisum ansvarar för fel eller brist i Tjänsterna som innebär att Tjänsternas innehåll eller funktion inte i väsentliga avseenden uppfyller Notisums vid var tid tillämpade tjänstebeskrivningar, och att felet eller bristen är hänförligt till Notisum. Notisum ansvarar inte för fel eller brister som är hänförliga till Licenstagaren, Användarna eller tredje man för vilken Notisum inte uttryckligen ansvarar.

8.3. Då Tjänsterna är beroende av internet är Licenstagaren införstådd med att avbrott, fördröjningar, buggar och liknande hinder mellan Tjänsterna och Användaren, såsom på internet, inte utgör fel i Tjänsterna.

8.4. Vid fel eller brist i Tjänsterna som inte avhjälpas inom skälig tid och som innebär att Användarnas användning av Tjänsterna påverkas väsentligen negativt har Licenstagaren rätt till skäligt prisavdrag från felanmälan till dess felet eller bristen avhjälpas. Om felet eller bristen är väsentligt och inte avhjälpas inom en skälig sista frist, har Licenstagaren rätt att säga upp Abonnemangsavtalet helt eller i berörda delar. Detta tillsammans med bestämmelserna i punkten 11 reglerar uttömmande Notisums ansvar vid fel eller brist i Tjänsterna.

9. Betalning

9.1. Licenstagaren är skyldig att erlägga avtalade, eller i annat fall vid var tid gällande, avgifter för all användning av Tjänsterna.

9.2. Notisum har rätt att höja avgift med omedelbar verkan om höjningen är direkt hänförlig till externa faktorer såsom förändring av valutakurs, skatt eller liknande allmän pålaga samt vid annan liknande omständighet av ekonomisk betydelse för Tjänst utanför Notisums kontroll och som påverkar kostnaden för tillhandahållande av Tjänst. Om inte annat följer av dessa allmänna villkor ska Notisum avisera avgiftsändringar som inte är att hänföra till externa faktorer senast trettio (30) dagar innan avgiftsförändringar träder i kraft, varvid Licenstagaren har möjlighet att säga upp Abonnemangsavtalet med trettio (30) dagars uppsägningstid.

9.3. Avgift för abonnemang erläggs i förskott mot faktura med betalningsvillkor trettio (30) dagar netto från fakturadatum. Eventuella särskilda avgifter för anslutning till och användning av vissa typer av Tjänster erläggs i efterskott mot faktura med nyss nämnda betalningsvillkor.

9.4. Vid dröjsmål debiteras lagstadgad dröjsmålsränta från förfallodagen. Vid betalningspåminnelse debiteras påminnelseavgift. Vid betalningsdröjsmål har Notisum rätt att tillfälligt stänga av Användares tillgång till Tjänsterna till dess samtliga förfallna belopp erlagts och/eller säga upp Abonnemangsavtalet till upphörande fjorton (14) dagar efter betalningspåminnelse.

9.5. Samtliga belopp i Abonnemangsavtalet och Notisums prislista anges exklusive moms. Kunden ansvarar för mervärdesskatt, andra skatter och offentliga avgifter som utgår eller kan komma att utgå med avseende på Tjänsterna.

9.6. Vid uppsägning sker ingen återbetalning av redan inbetald fast avgift förutom vid uppsägning enligt punkterna 8.4, 14.3 och 16. Kund är vid uppsägning skyldig att erlägga eventuella särskilda utgifter som faktureras i efterskott till Notisum i enlighet med punkten 9.3.

10. Force majeure

10.1. Ingen av parterna är ansvarig gentemot den andra parten för fullgörande av skyldigheter, enligt Abonnemangsavtalet eller dessa allmänna villkor, som förhindras av omständigheter utanför parts eller dennes leverantörs kontroll ("**Force Majeure**"), innefattande men inte begränsat till krig och mobilisering, naturkatastrofer, epidemier, lockout eller annan arbetskonflikt, brist på naturtillgångar, brand, skada på utrustning som används, ändrade myndighetsbestämmelser, myndighetsingripanden, avbrott i den allmänna samfärdseln, innefattande bland annat energiförsörjning och datavirus i Tjänsterna, samt import- och exportförbud och andra förbud utanför parts kontroll.

10.2. Det åligger part som önskar åberopa Force Majeure att utan uppskov skriftligen underrätta den andra parten om uppkomsten därav samt dess upphörande.

10.3. Om Abonnemangsavtalets fullgörande och uppfyllande av dessa allmänna villkor omöjliggörs under nittio (90) dagar på grund av Force Majeure har vardera part rätt att genom skriftligt meddelande till den andra parten häva Abonnemangsavtalet.

11. Ansvarsbegränsning och reklamation

11.1. Licenstagaren ska ersätta Notisum för skador som Notisum åsamkas på grund av att Licenstagaren och/eller Användare använder Tjänsterna i strid med Abonnemangsavtalet och dessa allmänna villkor eller på sätt som skadar Notisum.

11.2. Utöver vad som anges ovan under punkten 8 har Notisum inte något ansvar för Tjänsternas funktion eller kvalitet. Notisum svarar inte för sak- eller faktafel i Tjänsterna eller för de skador som kan uppstå med anledning därav. Inte heller ska Notisum ansvara för råd eller information som Licenstagaren eller Användare har beretts möjlighet att erhålla från av Notisum anställd konsult eller tredje part i anslutning till Tjänsterna.

11.3. Notisum har inget ansvar för produktionsbortfall, utebliven vinst, förlorad inkomst, följdskador eller annan indirekt skada eller förlust.

11.4. Notisums sammanlagda ansvar gentemot Licenstagaren är, utom i fall av grov vårdslöshet eller uppsåt, begränsat till den ersättning som Notisum erhållit under de senaste tolv (12) månaderna från Licenstagaren enligt Abonnemangsavtalet. Notisum ansvarar inte gentemot någon annan än Licenstagaren, såsom t.ex. Användarna, Licenstagarens kunder, leverantörer eller samarbetspartners eller myndighet som övervakar Licenstagaren.

11.5. Reklamation och andra anspråk ska framställas skriftligen och utan oskäligt dröjsmål från det att part upptäckt eller bort upptäcka den omständighet som föranleder anspråket, dock senast inom sex (6) månader från det att omständigheten inträffade, varefter anspråket annars förfaller.

12. Kunddata

12.1. Notisum har inte rätt att använda data som Licenstagaren, själv eller genom Användare, överlämnar till Notisum eller som Notisum annars får del av genom Licenstagarens användning av Tjänsterna ("**Kunddata**") om inte annat anges i dessa allmänna villkor.

12.2. Notisum får använda Kunddata för att fullgöra uppdraget, för statistiska ändamål samt för att förbättra och utveckla Notisums Tjänster.

12.3. Notisum får även överföra Kunddata till koncernbolag och leverantörer om det är nödvändigt för att kunna leverera eller utveckla Tjänsterna.

12.4. Licenstagaren ska se till att Kunddata är fri från virus, trojaner, maskar eller annan programvara eller kod som kan skada Tjänsterna eller Notisums IT-miljö.

13. Immateriella rättigheter

13.1. Dessa allmänna villkor medför inte att upphovsrätt eller andra immateriella rättigheter till Tjänsterna överläts till Licenstagaren, Användare eller annan tredje man. Licenstagaren och Användaren får inte kopiera, ändra eller på annat sätt hantera programvara eller annat material som hör till Tjänsterna, inte heller överlåta eller upplåta rätt till sådan programvara eller material till annan, om det inte följer av dessa allmänna villkor eller i övrigt skriftligen har avtalats med Notisum.

13.2. Licenstagaren åtar sig att på egen bekostnad försvara Notisum om krav riktas eller talan förs mot denna om intrång på grund av Licenstagarens eller Användares användning av Tjänsterna i strid med

dessa allmänna villkor. Licenstagaren åtar sig vidare att ersätta Notisum för alla de kostnader och skadestånd som Notisum genom förlikning eller dom kan bli skyldig att utge.

14. Avtalstid

14.1. Abonnemangsavtalet gäller, om inte annat avtalats, från undertecknandet och därefter under tolv (12) månader.

14.2. Om Abonnemangsavtalet inte sagts upp senast sextio (60) dagar före avtalstidens utgång, genom att Licenstagaren senast vid denna tidpunkt underrättar Notisum om uppsägningen, förlängs Abonnemangsavtalet automatiskt med tolv (12) månader, eller den förlängningstid som avtalats, med motsvarande uppsägningstid. Vid förlängning av Abonnemangsavtalet tillämpas Notisums vid var tid gällande allmänna villkor och priser. Uppsägningen ska vara skriftlig.

14.3. Utöver vad som i övrigt anges i Abonnemangsavtalet och dessa allmänna villkor har part rätt att med omedelbar verkan säga upp Abonnemangsavtalet om motparten (a) begått avtalsbrott och underlåter att vidta rättelse inom tjugo (20) dagar från mottagande av andra partens skriftliga erinran om avtalsbrottet eller (b) inleder likvidationsförfarande, ansöker om eller försätts i konkurs, ställer in betalningarna eller på annat sätt kan befaras vara på väg mot obestånd.

14.4. Från och med dagen för Abonnemangsavtalets upphörande har Licenstagaren inte längre någon rätt att använda Tjänsterna. I den mån Notisum har lagrat Resultat från Användarna eller annat material i anslutning till Tjänsterna har Notisum rätt att efter nittio (90) dagar från att Abonnemangsavtalet upphört radera sådant material.

15. Sekretess

15.1. Med "**Konfidentiell Information**" avses varje uppgift av ekonomisk, teknisk, kommersiell eller annan art hänförlig till parterna och deras närstående bolag, oavsett om uppgifterna dokumenterats i skrift eller inte. Som Konfidentiell Information ska dock inte betraktas information som är allmänt känd eller kommit till allmän kännedom på annat sätt än genom mottagande parts brott mot dessa allmänna villkor.

15.2. Parterna förbinder sig att inte helt eller delvis avslöja Konfidentiell Information, som erhållits i samband med Abonnemangsavtalet och dessa allmänna villkor, hänförlig till den andre parten eller till tredje man, om inte den andre parten i förväg har givit sitt skriftliga samtycke därtill eller den part som avslöjar den Konfidentiella Informationen har skyldighet att göra så enligt tillämplig lag, verkställbar dom, bindande myndighetsbeslut eller föreskrift eller tillämpligt regelverk för reglerad marknad. Parterna får inte använda Konfidentiell Information för annat ändamål än för att utöva sina rättigheter och skyldigheter enligt Abonnemangsavtalet och dessa allmänna villkor. Part ska vidta alla nödvändiga åtgärder för att förhindra att dess anställda eller uppdragstagare otillåtet sprider eller använder Konfidentiell Information.

15.3. Parternas sekretessförpliktelser ska gälla utan begränsning i tiden.

15.4. Notisum får, efter särskild överenskommelse med Licenstagaren, i marknadsföringssyfte ange att Licenstagaren är användare av Tjänsterna.

16. Ändring av allmänna villkor

Notisum har rätt att ändra dessa allmänna villkor utan föregående godkännande från Licenstagaren. Licenstagaren kommer att informeras om sådana ändringar som är till väsentlig nackdel för denne och sådana ändringar träder ikraft trettio (30) dagar efter det att Licenstagaren underrättats om ändringen. Vid ändringar som är till väsentlig nackdel för Licenstagaren har denne rätt att senast fjorton (14) dagar innan ändringens ikraftträdande underrätta Notisum om att Licenstagaren säger upp Abonnemangsavtalet till upphörande från och med dagen för ändringens ikraftträdande. Uppsägningen ska vara skriftlig.

17. Meddelanden

17.1. Notisum lämnar meddelanden till Licenstagaren via Tjänsterna, brev till den adress som Licenstagaren har meddelat, e-post till den e-postadress som Licenstagaren har meddelat eller på annat sätt som parterna kommit överens om.

17.2. Meddelande till Licenstagaren om villkorsändring och övriga eventuella meddelanden enligt dessa allmänna villkor, ska anses ha kommit Licenstagaren tillhanda senast tre (3) dagar efter det att meddelandet avsänts med post till den av Licenstagaren till Notisum senast skriftligen anmälda adressen. Meddelande som görs i Tjänsten eller som sänds via e-postmeddelande till den av Licenstagaren till Notisum senast anmälda e-postadressen ska anses ha kommit Licenstagaren tillhanda omedelbart.

17.3. Licenstagaren är skyldig att i Tjänsten meddela Notisum uppdateringar i sin adress, e-postadress eller andra kontaktuppgifter som lämnats till Notisum.

17.4. Licenstagaren kan lämna meddelanden till Notisum gällande dessa allmänna villkor genom att använda Notisums användarstöd i Tjänsterna.

18. Lagval och domsrätt

Svensk materiell rätt ska tillämpas på dessa allmänna villkor. Tvister hänförliga till dessa allmänna villkor ska prövas av Stockholms tingsrätt som första instans.

Annex 1 Data Processing Agreement

This Data Processing Agreement is between the Licensee, Data Controller, and Notisum, Data Processor, each a “Party” and collectively the “Parties”.

The parties HAVE AGREED on the following Standard Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1 Preamble

- 1.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
- 1.2 The Clauses have been designed to ensure the parties’ compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- 1.3 In the context of the provision of using Notisum’s internet services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 1.4 Four appendices are attached to the Clauses and form an integral part of the Clauses.
- 1.5 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- 1.6 Appendix B contains the data controller’s conditions for the data processor’s use of sub-processors and a list of sub-processors authorised by the data controller.
- 1.7 Appendix C contains the data controller’s instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
- 1.8 Appendix D contains provisions for other activities which are not covered by the Clauses.
- 1.9 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
- 1.10 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2 The rights and obligations of the data controller

- 2.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.
- 2.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
- 2.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3 The data processor acts according to instructions

- 3.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
- 3.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4 Confidentiality

- 4.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
- 4.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5 Security of processing

- 5.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- 5.2 The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
 - 5.3 Pseudonymisation and encryption of personal data;
 - 5.4 The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 5.5 The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - 5.6 A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 5.7 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
- 5.8 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.
- 5.9 If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6 Use of sub-processors

- 6.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
- 6.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.
- 6.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 3 months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.
- 6.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.
- 6.5 The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.
- 6.6 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
- 6.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7 Transfer of data to third countries or international organisations

- 7.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
- 7.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
- 7.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
- 7.4 Transfer personal data to a data controller or a data processor in a third country or in an international organization.
- 7.5 Transfer the processing of personal data to a sub-processor in a third country.
- 7.6 Have the personal data processed in by the data processor in a third country
- 7.7 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.
- 7.8 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8 Assistance to the data controller

- 8.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a The right to be informed when collecting personal data from the data subject
- b The right to be informed when personal data have not been obtained from the data subject
- c The right of access by the data subject
- d The right to rectification
- e The right to erasure ('the right to be forgotten')
- f The right to restriction of processing
- g Notification obligation regarding rectification or erasure of personal data or restriction of processing
- h The right to data portability
- i The right to object
- j The right not to be subject to a decision based solely on automated processing, including profiling

- 8.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

- a The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Swedish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- b The data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
- c The data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
- d The data controller's obligation to consult the competent supervisory authority, the Swedish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

- 8.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9 Notification of personal data breach

- 9.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
- 9.2 The data processor's notification to the data controller shall, if possible, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
- 9.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:
- a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
 - b. The likely consequences of the personal data breach.
 - c. The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 9.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10 Erasure and return of data

- 10.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11 Audit and inspection

- 11.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
- 11.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

- 11.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12 The parties' agreement on other terms

- 12.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g., liability, if they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13 Commencement and termination

- 13.1 The Clauses is an integrated part of the general terms of conditions and is valid from the acceptance of those.
- 13.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or in-expediency of the Clauses should give rise to such renegotiation.
- 13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
- 13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The Data Processor is delivering internet services to the Data Controller to support regulatory monitoring and handling legal compliance matters.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Notisum's internet services may be used to collect, process, and store personal information as part of the data controllers work with legal compliance matters. The Data Processor will only process personal data according to the Instruction from the Data Controller.

A.3. The processing includes the following types of personal data about data subjects:

The categories of personal data that are processed constitute all types of information that could potentially be relevant for handling compliance matters, e.g., personal data in connection with:

- a. identifying responsible natural persons for legal monitoring, auditing and other processes assisted by Notisum's internet services,
- b. storage of compliance audit proof documents and photos, permits and other internal documents,
- c. other information that appears from the content of data material that can be used in the process of regulatory monitoring and legal compliance audits.

The abovementioned list is a non-exhaustive list, and the data controller has the overall responsibility to ensure, that they have the right to process the personal data, which is uploaded to Notisum's internet services. The data processor does not control the types of documents and their content.

A.4. Processing includes the following categories of data subject:

The data subjects to whom the personal data relate will be parties who have or have had a relationship with the Data Controller and whose information is relevant to process by the Data Controller when conducting its process of regulatory monitoring and legal compliance audits, including among others

- a. management, employees, and advisors,
- b. parties who assist the Data Controller with tasks within the area of regulatory monitoring and legal compliance audits from a practical, technical, economic, or legal perspective,
- c. parties whose information may prove relevant in connection with the conduct of compliance audits, or
- d. information about parties who send or receive e-mails from the Data Controller, or whose information appears inside such e-mails, if such emails are store in Notisum's web services.

The abovementioned list is a non-exhaustive list, and the data controller has the overall responsibility to ensure, that they have the right to process the personal data, which is uploaded to Notisum's internet services. The data processor does not control the types of documents and their content.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The processing is not time-limited and lasts until the Clauses are terminated or terminated by one of the Parties.

Appendix B - Authorized sub-processors

B.1. Approved sub-processors.

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ORG NO:	ADDRESS	DESCRIPTION OF PROCESSING
Karnov Group Denmark A/S	10361990	Sankt Petri Passage 5, St. 1165 Copenhagen	E-mail handling and data storage. Karnov Group Denmark uses Microsoft Azure as cloud computing platform and data is stored on servers inside the EU (Microsoft West Europe (Netherlands) Microsoft North Europe (Ireland)).
Notisum ApS	36020156	Sankt Petri Passage 5, St. 1165 Copenhagen	Using the Notisum platform and content in Denmark
Echoline SAS	517886990	5, esplanade Compans Caffarelli – CS 57130 – Bâtiment A - 31071 TOULOUSE Cédex 7. FRANCE	Using the Notisum platform and content in France
DL Moberg AB	559132-7324	Vattenverksvägen 8, 184 33 ÅKERSBERGA	Database development and maintenance, customer support and customer implementation projects.
Mandoit AB	556063-8644	Sköldvägen 17. 187 36 TÄBY	Database development and maintenance, customer support and customer implementation projects.
Kopparklinten AB	556703-5612	Vindarnas väg 8, 42935 KULLAVIK	Database development and maintenance, customer support and customer implementation projects.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor's request for authorisation of a different sub-processor or change of processing activities must be received by the data controller at least 3 months prior to the application or change will commence. The data controller may only refuse approval if the data controller has reasonable, specific reasons for this.

Appendix C - Instruction pertaining to the use of personal data.

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor delivers Notisum's internet services, where personal information is collected, processed, and stored. The data processor may only process such personal data to the extent necessary to perform the tasks described in this appendix and the instructions documented by the data controller at any time.

The data processor is delivering the Notisum's internet services to the data controller to support the data controller's regulatory monitoring and handling of legal compliance matters.

C.2. Security of processing

The level of security shall take into account:

The nature, scope context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the data processor shall maintain an appropriate level of data security in accordance with best practice.

The Data Processor implements the following measures, which have been agreed with the Data Controller:

- a. At all times comply with the provisions described in the General Data Protection Regulation.
- b. Ensure the necessary technical and organizational measures against information being accidentally or illegally destroyed, lost, or impaired and that it comes to the knowledge of unauthorized persons, misused, or otherwise processed in violation of the General Data Protection Regulation.
- c. Protection of data where it is transmitted and stored. Data is encrypted in the transfer between the data controller and the data processor.
- d. Access to personal data is ensured only to relevant users
- e. The ability to ensure the ongoing confidentiality, integrity, availability and robustness of processing systems and services
- f. Using logging
- g. Remote security of premises where personal data is processed
- h. Perform annual risk assessments to determine if the agreed measures are sufficient.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 8.1. and 8.2. by implementing the following technical and organisational measures:

The data processor shall assess the need for, and to the extent necessary implement, processes that ensure assistance to the data controller in fulfilling its obligations to respond to requests for the exercise of the data subject's rights.

The data processor must assess the need for, and to the extent necessary implement, processes that ensure assistance to the data controller, with all the information available to the data processor that is needed for the data controller to assess the extent of the breach, report the breach to the supervisory authority and notify the data subjects.

In the event of a breach of personal data security, the following information must be submitted to the Data Controller:

Date and time:	The breach of personal data was detected on [date], at [time].
Circumstances of data breach:	The breach is due to [the circumstances of the breach of data security].
The character / nature of the breach:	At present, it is noted that [Insert information about the nature of the breach. As long as it is possible to determine the following: 1) Categories and the approximate number of data subjects involved 2) Categories and the approximate amount of personal data information involved.]
Other relevant information	At this point, it is noted that [Indicate other information about the breach of personal data that may be useful to the data controller's assessment of the impact of the breach].
Actions taken:	In order to limit the extent and consequences of the breach, we have so far [Measures taken by Notisum to address the breach of personal data, including measures taken to limit any harmful effects].
Point of Contact at the data processor:	[Contact information].

The information must be sent to the data controller's contact person as specified in clause 14 of the Clauses.

The data controller has the right at any time to request that answers be specified in the event of any questions of doubt.

C.4. Storage period/erasure procedures

Personal data is stored for up to 12 months after termination of the agreement after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall delete the personal data in accordance with Clause 10.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Notisum's internet services are hosted in Microsoft azure and are therefore located on Microsoft servers within the EU. Data is located at the datacentre Microsoft EU West in the Netherlands and some of the data is replicated at the datacentre Microsoft EU North in Ireland.

Microsoft Azure uses sub-processors the list can be found at https://aka.ms/Online_Serv_Subcontractor_List, who provides technologies to power or provide ancillary services to certain Microsoft Online Services, or who provides contract staff.

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

NAME	ADDRESS	DESCRIPTION OF PROCESSING	LEGAL BASIS FOR THE PROCESSING
Karnov Group Denmark	Microsoft West Europe (Netherlands) and Microsoft North Europe (Ireland)	E-mail handling and data storage. Karnov Group Denmark uses Microsoft Azure as a sub-processor. Data is stored on servers inside the EU and will generally not be transferred outside of the EU.	Standard Contractual Clauses (SCC) and supplementary measures.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor.

The data processor shall, at the request of the data controller, submit a management statement declaring the data processor's compliance with the data protection regulation, data protection provisions of other EU or national law and these Clauses.

The data controller may request additional information in the form of a written inspection with a questionnaire or using another method.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, on the premises from which the data processor performs the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary.

In addition to the planned inspection, the data controller may carry out an inspection at the data processor when the data controller deems it necessary e.g., in connection with handling breaches of personal data. Inspection visits can be made by relevant employees.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, on the premises from which the data processor performs the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary, but not without prior notification to the data processor.

In addition to the planned inspection, the data controller may carry out an inspection at the data processor, when the data controller deems it necessary, e.g., in connection with handling breaches of personal data. Inspection visits can be made by relevant employees after prior notification.

Any expenses incurred by the data controller in connection with a physical inspection shall be borne by the data controller itself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out his inspection.

The Data Processor is entitled to reasonable remuneration for documented time spent at the hourly rate stated in the main agreement, and costs associated with the assistance regarding the abovementioned inspections written, physical or otherwise, unless otherwise agreed between the Parties.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors.

The data processor is responsible for carrying out the necessary supervision of the sub-processors. Documentation of the performed inspection can be sent upon request, to the data controller.

Based on the results of the documentation submitted, the data controller is entitled to request the implementation of additional measures to ensure compliance with the GDPR, data protection provisions of other EU member states, or national law and this DPA.

The Data Processor is entitled to reasonable remuneration for documented time spent at the hourly rate stated in the main agreement, and costs associated with the assistance regarding the abovementioned inspections written, physical or otherwise, unless otherwise agreed between the Parties.

Appendix D - The parties' terms of agreement on other subjects

D.1 Derogation from standard clauses

The paragraph below, has been deleted from the standard contractual clauses and does not apply to this agreement.

The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g., enabling the data controller to instruct the sub-processor to delete or return the personal data.

D.2 Remuneration to the data processor

The Data Processor is entitled to reasonably and documented remuneration for time spend at the hourly rate stated in the main agreement, for documented and reasonable costs associated with changes and/or assistance to the Data Controller, unless otherwise agreed between the Parties.