Rekommendationer för GDPR

Visma Control Product Line

Visma Software AB

Dokumentrevision 2

Dokumenthistorik

Revision	Datum	Kommentar	Författare
0	2018-01-04	Första utgåva, på svenska	Daniel Zagar
1	2018-01-12	Reviderad efter granskning	Daniel Zagar
2	2018-01-15	Mindre korrigering	Daniel Zagar

Bakgrund

I maj 2018, kommer nya regler; GDPR, att träda ikraft inom EU, gällande hur personliga data ska hanteras inom digitaliserad informationsbehandling, vilket får genomslagskraft för alla verksamheter som på något sätt hanterar data om enskilda individer (privatpersoner).

Visma sätter stort fokus kring detta område, och prioriterar högt att kunna stödja våra kunder för att på ett så enkelt sätt som möjligt kunna tillmötesgå kraven. Detta dokument redovisar de viktigaste områdena för mjukvarorna inom Visma Control Product Line (VCPL), gällande vad du behöver tänka på för att du som kund ska kunna tillmötesgå GDPR.

Syfte

Dokumentet är avsett som en hjälp, för att på ett så enkelt sätt som möjligt sätta upp en miljö som fungerar i enlighet med reglerna för GDPR. Dokumentet omfattar tips och saker man ska tänka på, men är inte ett uttömmande regelverk, och ska inte användas som ett acceptans-underlag eftersom de precisa förutsättningarna för hur GDPR kan uppfyllas varierar från miljö till miljö. Det beror också på vilken typ av data man hanterar i systemet, och vad systemet är avsett att användas för, samt syftet till varför visst data lagras, så kallad uppgiftsminimering. Uppgiftsminimering åligger varje kund att själv beakta, eftersom kunden äger sitt data.

Omfattning

Dokumentet täcker aspekterna kring GDPR, för en standardmiljö av produkterna i VCPL, dvs:

- Visma Control och Visma Reporting
- Visma DCE
- Visma PX

Dessutom ingår normalt anslutningar till andra Visma-baserade system; typiskt system som utnyttjar tjänsterna i Visma On Demand Platform (ODP), dvs Autopay och Approval. Aspekterna kring GDPR för dessa system är emellertid *inte* inkluderade i detta dokument.

För tjänsterna utanför Visma Control PL, är aspekter kring GDPR och säkerhet beskrivet i:

https://www.visma.com/privacy/ https://www.visma.com/trust-centre/

Observera

Produkterna inom VCPL är avsedda att användas i en så kallad on premise-miljö. Det innebär att du som kund äger och ansvarar för den miljö som mjukvarorna från Visma ska köras i, och att du som kund även har det yttersta ansvaret för att tillmötesgå kraven för GDPR. Detta är helt likvärdigt med de juridiska krav som redan i dag gäller för hantering av finansiella data, dvs t ex bokföringslagen och regler och lagar kring skatt och moms. Icke desto mindre försöker Visma leverera lösningar som i så stor utsträckning som möjligt kan underlätta för dig som kund att tillmötesgå kraven, och detta gäller naturligtvis även aspekterna kring GDPR.

Generella aspekter

Användning av data

Alla data där dess huvudsakliga syfte frångås, kan leda till att man åsidosätter GDPR. Detta gäller inte bara fält och kolumner som har ett förbestämt syfte, utan också på ställen där det finns möjligheter att lagra godtycklig information. Fritextfält och kommentarer är källor till sådana missbruk, och dessa kan också ha ett innehåll som är särskilt svårt att söka på och analysera.

Lagring av data

För systemen i VCPL, lagras data på olika ställen och i olika former. För ett system som är under drift är det normalt att data förekommer åtminstone på följande ställen:

- I systemens databaser
- I loggfiler på serversystem
- I loggfiler på lokala klientmaskiner
- Arkivfiler, t ex bildfiler över fakturor
- I cookies av olika slag, där inbäddade webb-fönster förekommer i klienten
- I cookies av olika slag, där en vanlig webbläsare används

Anpassningar av olika slag kan dessutom eventuellt lagra sina unika data på andra ställen. Avarter och varianter av dessa data, som skapas av ett körande system, är också mycket vanligt förekommande:

- Direkta säkerhetskopior, dvs av databaser eller vanliga filer, t ex ett bildarkiv över fakturor, där man sparat detta material på särskilt avsedd plats.
- Indirekta säkerhetskopior, t ex filer som lagrats i en molntjänst, t ex DropBox eller Google Drive. Här har man i princip ingen som helst kontroll över vilken spridning av data som förekommer, vare sig för data i drift eller för data som leverantören av lagringstjänsten har säkerhetskopierat.

Observera att för samtliga av dessa data står du som kund som ansvarig, och här gäller reglerna för GDPR oavsett om data spridits i ett normalfall, eller om det skett i form av en otillåten operation, incident, t ex att någon kopierat en säkerhetskopia av en databas och sedan skickat den för analys eller support hos en utomstående aktör.

Överföring av data

Mjukvarorna inom produktlinjen interagerar sinsemellan, och delar data på olika sätt. Men i typiska miljöer vill man också interagera med andra, yttre, system. Dessa kan vara andra system från Visma som erbjuder utökade funktioner, t ex Autopay och Approval, men även system från tredjepartsleverantörer.

Så fort data flödar över gränsen för mjukvarorna i VCPL, kan den GDPR-mässiga integriteten för dessa data inte täckas av detta dokument, utan man måste följa de direktiv som dessa system i sin tur postulerar. Observera också att data, som i VCPL-miljön kan vara skyddade av olika integritets- och behörighetssystem, inte nödvändigtvis besitter samma skydd när de överförts till ett yttre system.

Support

I en icke försumbar mängd supportärenden som ska hanteras av en utomstående aktör (betraktat ur dataägarens synvinkel, i det här fallet t ex Visma), måste skarpa data från systemet bifogas det material som skickas vidare för analys. Typiskt är att i ärendet, utöver beskrivningar av hur beteenden ska reproduceras, man också skickar med konfigurationsfiler för systemet, samt själva databasen (som en offline-fil). Detta är i det generella fallet inte tillåtet, även om supportagenten är Visma själv. Särskilda avtal måste upprättas mellan dig som kund och Visma, för att du ska tillåtas att skicka sådan information utanför ditt företags gränser, och specifika regler gäller för hur denna data får hanteras.

Återkallande av personliga data

Då syftet med en datalagring av en individ (subjekt) har upphört att vara gällande, kan subjektet begära att lagringen av data om denne återkallas, dvs att man kan radera alla huvud- och underposter som sparar data om subjektet, eller avidentifiera. Detta förutsätter naturligtvis att bokföringslagen fortfarande tillämpas tillfyllest:

- Bokföringsunderlag som är äldre än 10 år
- Fakturaunderlag som är äldre än 7år

Raderingen, eller avidentifieringen, av sådana data kan utföras i form av konsultuppdrag, t ex vid årsavslut eller uppgraderingar. För detta syfte finns ett åtgärdspaket framtaget – ”GDPR- och rensningspaket” – vilket kan levereras av konsultavdelningen, och tillämpas på samtliga produkter i produktlinjen.

För att få detta utfört, samt prisuppgift, vänligen kontakta er kundansvarig.

Appendix 1: Visma Control

Funktioner som påverkas av GDPR

För standardmässigt innehåll i Control, som på ett direkt sätt kan associeras med enskilda individer, kan sådant förekomma i:

- Leverantörsregistret
  Det kan förekomma att en leverantör är en enskild individ, beroende på att man vill hantera utbetalningar knutna till denna person. Det kan också förekomma att man har anteckningar kring enskilda individer i leverantörsregistret.
- Kundregistret
  Här kan det förekomma att en kund direkt kan vara en enskild individ, men också som i fallet med leverantörer, att det finns anteckningar kring en enskild individ, sparat i kundregistret.
- Kontaktlistor
  Förekommer både bland kunder och leverantörer

Dessutom är det vanligt att man i indirekta förteckningar sparar data som kan associeras med enskilda individer:

- Kontoförteckning
  Här kan det förekomma konton som kan associeras med individer, typiskt lönekonton där man i förekommande fall vill knyta ett enskilt lönekonto till en enskild individ.
- Objekt
  Detta är en konfigurerbar del av Control, där kunden själv bestämmer vad olika objekt ska representera. Här kan det alltså förekomma att en viss objekttyp kommer att representera känslig information kring en enskild individ. T ex ett personnummer.

För samtliga av dessa register måste alltså kraven på GDPR vara uppfyllda.

Funktioner som direkt stödjer GDPR

I samband med releasen av Control 10.10, erbjuds ett antal funktioner som vi rekommenderar att sätta i bruk för att tillmötesgå GDPR:

1. Loggning
2. Behörighetskoder och privilegier
3. Rapport för dataspårning
4. Anpassade inställningar i installationen
5. Dokumentation (detta dokument; för rekommendationer och tillämpning)

Det kan också i förekommande fall finns uppdateringar i eventuella anpassningar som är unika för en viss kund.

Nedan beskrevs respektive funktion i mera detalj.

1 Loggning

Det finns en loggningsfunktion, där det går att spåra och dokumentera vilka ändringar som gjorts, och av vem. Dock finns ingen inbyggd spårning av *läsningar* av data.

2 Behörighetskoder och privilegier

Visma Control är sedan länge uppbyggt kring ett ramverk för styrning av åtkomst och behörigheter, i flera olika nivåer. Med hjälp av dessa, befintliga, mekanismer, kan man genom att dessa hanteras på korrekt vis, framställa ett system som till mångt och mycket tillmötesgår GDPR, t ex genom att använda behörighetskoder (UAC); se nedan. Systemet för behörighetsstyrning tillämpas dock enligt en mycket fundamental grundprincip: *Användare som ges administratörsrättigheter måste ges ett mycket högt förtroende*. Missbruk av detta förtroende kan medföra att denne användare kan traversera förbi i princip samtliga säkerhetsbarriärer i systemet, och detta dessutom utan att lämna spår efter sig.

Var alltså ytterst restriktiv med vilka användare som ges administratörsrättigheter, och det är rekommenderat att upprätta särskilda ansvarsavtal med dessa.

För varje storhetstyp som är relevant för skydd enligt GDPR, finns tre nivåer:

- Ingen åtkomst
- Åtkomst med enbart läsrättigheter
- Åtkomst med rättigheter att både läsa och ändra

Observera att tilldelning av läsrättigheter även medger möjligheten att kopiera data, och indirekt då också spridning av dessa data utanför systemet.

Man kan också på postnivå styra precist vilka poster som en viss användare ska ges åtkomst till, genom att tillämpa behörighetskoder (UAC). Enskilda rader i listor av bl a typen kunder, konton eller leverantörer kan markeras och förses med särskilda behörigheter, där det krävs en behörighetskod för att överhuvudtaget få se de aktuella posterna. Observera att i de fall man lägger till nya poster, måste denna operation utföras manuellt, innan posten blir skyddad.

3 Rapport för dataspårning

Under funktionsgruppen rapportering, finns särskilda rapporter utformade för att underlätta redovisning av GDPR-relaterade data.

I Control 10.10 hittar man detta i utskriftscentralen på följande ställe:

Kund- eller leverantörsreskontra – Månadsrapporter – Information om personuppgifter

4 Anpassade inställningar i installationen

Olika scenarier för konfiguration

Genom sin natur, tillhandahåller Visma Control en stor flexibilitet för konfiguration och anpassningar, men denna flexibilitet måste också noggrant beaktas, så att man inte konfigurerar ett system som kan tänkas bryta mot reglerna i GDPR.

Det finns förutom fast definierade data-tabeller, även storheter där användaren själv kan definiera vad innehållet ska betyda:

- Objekt (redigeras som objekttyper)
- Grupper (redigeras som grupptyper)

För dessa kan man i princip definiera helt fritt vad dessa ska ha för innebörd i det aktuella systemet, vilket medför att det även går att definiera storheter vars lagring och hantering av tillhörande data, inte kan anses vara i enlighet med GDPR.

Exempel; objektuppsättning som är fullt godtagbar:

- Objekt 1 = Projektnummer
- Objekt 2 = Produktionslinje

Exempel; objektuppsättning som inte utan särskild anledning får användas för att spara data:

- Objekt 1 = Sexuell läggning
- Objekt 2 = Sjukdomar i släkten

Observera att det endast rent strikt är när det finns data associerade till dessa objekt, som hanteringen kan vara föremål för missbruk av GDPR.

Anpassningar

Eftersom arsenalen av funktioner som kan iscensättas med en anpassning till Control, i princip är obegränsade, kan det inte inom ramarna för detta dokument fastställas hur anpassningar ska implementeras och hanteras för att uppfylla kraven för GDPR. Som beställare och kund kan man kräva att varje anpassning redovisar hur denna tillmötesgår kraven på GDPR.

Installation och anpassningar i det lokala filsystemet

Med lokalt filsystem menas de lagringsutrymme som finns på en viss dator, och data som sparas enbart för lokal åtkomst i denna miljö. Två slags integriteter måste upprätthållas:

- Skydd mot oavsiktlig läsning, även inkluderande otillåten kopiering
- Skydd mot manipulation

I Visma Control version 10.10 finns ingen automatisering av hur säkerhetsnivåer för lokala filer ska hanteras, men man kan om man har administratörsrättigheter i NTFS-filsystemet göra vissa justeringar som underlättar att dessa integriteter bibehålls.

Filer	**Rekommenderad säkerhetsnivå**	**Kommentar**
AppDefault.cxml	Enbart läsning[1]	Om användaren får ändra i denna fil kan man ges åtkomst till högre behörigheter än förväntat.
Loggkatalogen	Endast åtkomst för de processer som sparar data här	Reguljär användare behöver i normala fall inte ges åtkomst till denna katalog. Vid supportärenden kontaktas i så fall administratören
App.config	Enbart läsning[1]	
Katalogen Plugins	Enbart läsning[1]	
Rapporter	Endast åtkomst för de processer som bearbetar rapporter på servern	
Exportfilter	Endast åtkomst för de processer som bearbetar export på servern	

[1] Enbart läsning innebär att man sätter NTFS-rättigheterna till Read Only. Dvs den ordinära funktionen ”Skrivskydd” i filegenskaper ska inte användas.

Appendix 2: Visma DCE

Personlig information som hanteras i systemet

Data som kan användas till att identifiera en enskild individ eller som avser en enskild individ, definieras som personlig data. Nedan beskrivs vilken personlig data som hanteras i Visma DCE.

Följande data är obligatorisk och lagras i användarregistret i DCE.

- Användar-ID (login)
- Namn (fullständigt namn kopplat till ett användar-ID)
- Lösenord (Obs! Om Windows autentisering används är inte detta relevant.)
- E-postadress

Ovan angivna data lagras också i relation till andra typer av data i samband med att olika funktioner används. Se vidare nedan under rubriken ”Hur används den personliga informationen?”.

Personliga data kan även registreras i andra, icke obligatoriska, fält i systemet. Detta gäller t ex

- Referens
- Avtalstecknare
- Kontaktperson för leverantörer
- E-postadress för påminnelse

Utöver ovan nämnda fördefinierade datafält kan det förekomma personliga data i fält där innehållet definieras av kunden eller användaren själv, t ex

- Fria fält relaterade till ett avtal
- Objekt som används vid kontering, där ett objektvärde kan kopplas till en enskild person
- Meddelande på en faktura

Hur används den personliga informationen?

Import av användare

DCE stödjer import av användare från Windows Active Directory (AD). I det fall att denna funktion används förs följande data över från AD:

- Användar-ID
- Förnamn
- Efternamn
- E-postadress

Om ovanstående information uppdateras i AD efter att import gjorts till DCE görs ingen synkronisering med automatik.

Import av faktura

Vid import av fakturadata kan personliga data i form av en referens förekomma. Referensdata används för att adressera en faktura till en viss mottagare för vidare handläggning.

Säkerhet

Personliga data används för att hantera autentisering då autentisering via ”Forms” används, samt för tilldelning av behörigheter och rättigheter i DCE.

Fakturaåtgärder
Vid hantering av en faktura används personliga data för att registrera att en viss person har utfört en viss åtgärd, t ex kontering, sakgranskning, attest eller utanordning.

Fakturaflöde
Personliga data används för att registrera avsändare och mottagare av en faktura.

För att kunna följa upp en fakturas flöde genom systemet registreras personliga data relaterat till olika händelser.

Meddelande
Användarmeddelanden registreras i relation till den användare som skapar meddelandet.

Bilagor
Bilagor registreras i relation till den användare som lägger till bilagan.

Avtalshantering
Vid registrering av ett avtal används personliga data för att koppla en ägare till avtalet. Personliga data används även för att registrera vem som skapat samt uppdaterat ett avtal.

Avisering
Personlig information används vid olika typer av aviseringar via e-post, t ex för att meddela att det finns en faktura att hantera eller påminna om ett avtal som kräver en åtgärd.

Logg vid registerändringar
Vid registerändringar används personliga data för att registrera vem som utfört ändringen.

Delning av data med Control
Från Control finns möjlighet att öppna en vy som visar fakturainformation från DCE. Inga personliga data förs dock över från DCE till Control.

Skydd av personlig information

Behörigheter och rättigheter
Genom att tilldela behörigheter och rättigheter i DCE går det att styra vilken data en användare har åtkomst till samt vilka funktioner en användare har tillgång till.

För att kunna se och uppdatera personlig information krävs specifika administratörsrättigheter.

Andra exempel är sekretessfunktion samt sökrättigheter i olika nivåer. Genom att sekretessmärka en faktura kan endast användare med tilldelad rättighet se fakturadokumentet. Genom tilldelning av sökrättigheter kan man begränsa vilka fakturor en användare kan se i systemet.

Kryptering
Vi rekommenderar att kommunikation mellan webbläsare och webbserver krypteras, d v s att kommunikationen sker via https-protokollet. I synnerhet gäller detta då kommunikation sker över internet.

Om en extern smtp-server används för utskick av e-post rekommenderar vi att kryptering används för kommunikationen mellan klient och server.

Loggfiler
DCE sparar eventuella felmeddelanden samt annan information, exempelvis för möjliggörande av felsökning, i textfiler på serversidan. Filerna kan innehålla personlig information som exempelvis

användar-ID eller e-postadress. Dessa filer är icke krypterade textfiler som normalt sparas under mappen där DCE finns installerat. För att begränsa åtkomst till dessa filer kan man använda rättighetssystemet för Windows filsystem och endast ge access till behöriga användare. För att DCE ska fungera behöver DCE:s systemanvändare skrivrättigheter under installationsmappen för DCE.

Övrigt

Personlig information bör inte anges i ”fria fält”, t ex meddelanden, för att undvika att personliga data lagras utom kontroll.

Tillgång till personlig information

Namn samt e-postadress som är registrerat för en användare visas efter inloggning längst upp till höger i DCE:s webbapplikation. Dessa personuppgifter kan inte uppdateras av användaren själv. För korrigering görs begäran om detta till den lokala systemadministratören.

Lösenord

Lösenord kan användaren själv ändra via menyn inställningar som nås längst upp till höger i webbapplikationen. Om en användare glömmer sitt lösenord får användaren begära ett nytt av den lokala systemadministratören. Nya lösenord är tillfälliga och måste ändras vid första inloggning.

Förfrågan om personuppgifter

Det finns stöd i DCE, från och med version 10.10.0, att vid förfrågan från en enskild person om vilka personuppgifter om hen som finns lagrade i DCE, ta ut en rapport om detta. Denna rapport är i PDF-format.

Ta bort personlig information

Användare tas bort via DCE:s administratörsapplikation. För att ta bort användare krävs specifika rättigheter.

I samband med att en användare tas bort från användarregistret raderas även följande typer av data relaterad till användaren

- Användarinställningar
- Rättigheter
- Konteringsbehörigheter
- Sökbehörigheter
- Attestbehörigheter
- Attestundantag
- Koppling till referens
- Personliga konteringsmallar
- Koppling till affärsenheter
- Koppling till roller

Personlig information kommer efter radering enligt ovan högst troligt att finnas kvar i andra register i systemet i form av t ex attestsignaturer, i historikloggar eller som avtalsägare. Detta för att inte bryta mot lagar och regler för bokföring och spårbarhet. För att ta bort historiska data som inte längre behöver sparas av juridiska skäl krävs en manuell åtgärd.

Anpassningar

Vid eventuella anpassningar där personlig information hanteras behöver hänsyn tas till GDPR. Som beställare och kund kan man kräva att varje anpassning redovisar hur denna tillmötesgår kraven på GDPR.

Appendix 3: Visma PX

Funktioner som påverkas av GDPR

Visma PX är en produkt som håller ett register över sin personal och som används av samtliga anställda på företaget, även många underkonsulter. Bland andra funktioner innehåller systemet tidrapportering där respektive anställd anger vad de har lagt sin tid på inklusive frånvaro ex. sjukdom för tidstatistik och överföring till lönesystem.
Det finns även en valfri möjlighet att registrera de anställdas hemadresser då det påverkar resetraktamente enligt norska bestämmelser.
Detta och annat gör att systemet innehåller data som påverkas av GDPR.

Då Visma PX alltid körs med Visma Control för ERP-delarna gäller också alltid det som listas under Appendix 1.

Funktioner som direkt stödjer GDPR

Från och med PX Version 10.01 kan inloggad användare via menyvalet Personligt data i Visma PX under Eget se vilket data som finns registrerat i personalregistret som gäller hen.
Inloggad användares anställnings-ID är förifyllt som parameter till rapporten men kan ändras till att visa data för någon annan, dock under förutsättning att den inloggade användaren har attestgruppsrättighet att läsa personaldata för angiven anställd. Detta ger möjlighet att skriva ut data t.ex. för tidigare anställda personer.
Det är möjligt att ange kontaktuppgifter i webbinställningarna om vem man kan kontakta, eventuellt telefonnummer och eventuell e-postadress. Då dessa uppgifter anges i webbinställningarna är det möjligt att ha olika kontaktinformation för anställda och underkonsulter.

Samtliga tabellposter i databasen loggar uppgifter om vem som *senast* sparade posten och tidpunkten då det skedde. På uppdragstransaktioner loggas samtliga förändringar gällande vems som gjorde det och när.

Hantering av behörigheter och åtkomst

Då Visma Control används för ERP-funktionaliteten i Visma PX gäller det systemets förutsättningar även Visma PX. Var god läs igenom den texten om detta inte redan är gjort då den informationen inte kommer att upprepas här.

Definitionen av hur och till vad objekten och grupperna skall användas och hur de påverkar GDPR gäller även för Visma PX. Den enda skillnaden är att de fem första objekten har fått en bestämd användning:

- Objekt 1 = Kostnadsställe (Enhet/ Avdelning)
- Objekt 2 = Ändamål (dvs vad verifikation avser)
- Objekt 3 = Företagskod (för mellanhavanden i stora bolag)
- Objekt 4 = Anställnings-ID
- Objekt 5 = Uppdrags-ID

Då Visma PX ända från början är byggt för att användas av samtliga anställda på företaget är mycket fokus satt till säkerhet runt åtkomst av funktionalitet och data. Det räcker inte med att en användare får öppna ett visst formulär eller en viss rapport, systemet kommer säga ifrån om rättigheten saknas att se en viss enhet, anställd, uppdrag etc. och i listor visas endast de poster användaren får se.

För att kunna sätta upp dessa rättigheter korrekt för varje användare definieras rättigheterna på användare/anställd-nivå och inte på rollnivå. För att underlätta kan man dock ta hjälp av mallar.

Rättigheterna tilldelas anställda/användare i huvudsak inom fyra områden:

Funktionsbehörigheter

Nivå av rättighet för en viss funktionalitet ex. Uppdrag (Ingen/Läs/Normal (skriv)/Admin).
Dessa rättigheter administreras i gränssnittet för underhåll av användare i Visma Control

Rapportgruppsbehörigheter

Alla rapporter och grafer i Visma PX kopplas till en av de rapportbehörighetskategorier som respektive bolag definierar själva. Varje anställd/användare tilldelas sedan rätten att använda rapporter och grafer genom att vissa rapportbehörighetskategorier kryssas för.

Resultatenhetsbehörigheter

Förutom att kostnadsställen/enheter, som är definierade som valida förekomster i objekt1 är det möjligt att definiera aggregeringsnivåer byggda på dessa enheter i Visma PX att använda vid de flesta typer av uppföljningar i systemet. Det kan vara att en chef vill följa upp sina två enheter som en, att regionchefen vill se sitt resultat med drill-down möjligheter eller att ekonomichefen och andra i ledningsgruppen vill ta sig en titt på hela företaget.
Dessa uppsummeringsenheter definieras som urvalsprofiler för andra enheter t.ex. 5201+5202, 6% (alla enheter som börjar på 6) osv.
Man tilldelar sedan anställda rättigheten att se data för resultatenheter på samma sätt med urvalsprofiler.

Attestgruppbehörigheter

Känsligare data styrs av så kallade attestgruppsrättigheter. Det kan tyckas att man borde kunna använda profileringen av resultatenheter för att tilldela dessa rättigheter men för att inte tilldela för breda rättigheter runt känsligare data för att man vill ge läsåtkomst till annat data är det uppdelat i Visma PX. Alla anställda och alla uppdrag kopplas till en attestgrupp. På varje anställd kan man sedan kryssa för vilka rättigheter hen skall ha för anställda/uppdrag kopplade till en viss attestgrupp. Exempel på rättigheter är olika typer av attesteringar, rätten att se personliga data, rätten att ändra finansiellt påverkande data efter det att ett uppdrag blivit attesterat etc.

Förutom det nämnda finns det en mängd andra styrningar och systeminställningar som kan påverka t.ex. att uppdragsledare får se och jobba med sina egna uppdrag, att en användare är uppdragsledare för det samfaktureringsuppdrag som det aktuella uppdraget tillhör osv.