

HOOFDSTUK 4 Automatisering en toezicht

Open vragen

Opgave 4.1

1. De gevolgen van toepassing van ESS en MSS voor de HR-afdeling van Burger Vormgeving vof:
 - Doordat medewerkers zelf hun gegevens aanpassen, zullen deze gegevens minder fouten bevatten.
 - Alle relevante HR-informatie is voor iedereen inzichtelijk en toegankelijk.
 - E-HRM maakt de HR-processen helder en doorzichtig.
 - Via het gebruik van e-HRM zijn veel administratieve werkzaamheden op de HR-afdeling niet langer nodig.
 - De administratieve werkzaamheden veranderen in controlewerk en krijgen een meer strategische aard.
 - De gegevens zijn actueler, zodat het management beter en gemakkelijker geadviseerd kan worden over de koers van HR in de onderneming.
 - Met behulp van dashboards kunnen de ken- en stuurgetallen van de diverse afdelingen worden gepresenteerd.
2. Outsourcing (uitbesteding) is een totaaloplossing. De continuïteit van de salarisadministratie wordt gewaarborgd door goede bereikbaarheid, back-ups van de gegevens en administratie en de kennis die de specialist over de onderneming opbouwt. Bij de uitbesteding van de salarisadministratie heeft een onderneming in veel gevallen vrijheid in de manier waarop zij de mutaties aanlevert. Of het nu gaat om mail of eigen online software, de dienstverlener zal zich door de gespecialiseerde werkzaamheden kunnen aanpassen aan de voorkeur van de klant.
3. Een oplossing hiervoor is single sign-on (SSO) software. SSO-software vangt alle inlogvensters van applicaties af en vult automatisch de gevraagde gebruikersnaam en het wachtwoord in. De eindgebruiker hoeft slechts één keer aan te melden met de gebruikelijke aanmeldprocedure op de computer.
4. Er is sprake van een datalek als derden die geen toegang zouden mogen hebben tot bepaalde persoonsgegevens, toch die informatie in handen krijgen.
5. De AVG is de opvolger van de oude Wet bescherming persoonsgegevens (Wbp).
6. Met de AVG moet een organisatie met alle leveranciers en afnemers een *verwerkersovereenkomst* sluiten. In deze verwerkersovereenkomst maken de partijen specifieke afspraken over de omgang met persoonlijke gegevens. Een belangrijk aandachtspunt daarbij is dat wanneer men diensten uitbesteedt waarbij persoonsgegevens van een klant zijn betrokken, men hiervoor dan ook toestemming nodig heeft van deze klant.
7. De traditionele vorm van aangifte doen en controleren kost de Belastingdienst, maar ook de andere betrokkenen zoals de ondernemer en diens adviseur, veel menskracht en is daarom ongewenst. Daarbij komt dat de Belastingdienst het meest gebaat is bij ondernemingen die altijd juist, volledig en tijdig afdragen wat zij aan belastingen verschuldigd zijn, zonder ingrijpen van de fiscus. Deze combinatie van factoren heeft geleid tot horizontaal toezicht door de Belastingdienst.

8. De leiding van Concern nv (= de ondernemer):
 - draagt zorg voor een systeem van interne beheersing, interne controle en externe controle met als doel het opstellen en indienen van aanvaardbare aangiften [die voldoen aan wet- en regelgeving en vrij zijn van materiële fouten];
 - zorgt voor het tijdig betalen van belastingschulden;
 - legt ingenomen of in te nemen relevante (fiscale) standpunten zo snel mogelijk voor aan de Belastingdienst. Het gaat daarbij om zaken waarover verschil van inzicht met de Belastingdienst kan ontstaan, door bijvoorbeeld een verschil in duiding van feiten of door wetsinterpretatie;
 - verstrekt aan de Belastingdienst actief inzicht in alle relevante feiten en omstandigheden, de standpunten en haar visie op de daarbij behorende rechtsgevolgen;
 - bevordert het werken in de actualiteit. Aangiften over een verstreken tijdvak worden zo spoedig mogelijk na het verstrijken van dat tijdvak ingediend. De door de fiscus gevraagde informatie wordt zo snel mogelijk, volledig en eenduidig verstrekt.
9. Een tax control framework (TCF) is een samenstel van processen en interne beheersingsmaatregelen (controls) dat ervoor moet zorgen dat de fiscale risico's van een bedrijf bekend zijn en beheerst worden. Een TCF is een belangrijk middel om de totale fiscaliteit binnen een organisatie te beheersen.

Een TCF omvat alle op de desbetreffende organisatie van toepassing zijnde belastingen, bijvoorbeeld vennootschapsbelasting, dividendbelasting, loonheffing, omzetbelasting, invoerrechten en accijnzen. Maar ook regulerende energiebelasting, kansspelbelasting, milieubelastingen, verpakkingenbelasting, BPM, vliegticketbelasting, enzovoort moeten in een TCF een plaats krijgen. Ook het volledig, juist en tijdig doen van aangiften en betalingen valt binnen het gebied van een TCF.
10. Een TCF is nooit afgerond. De organisatie en de omgeving zijn permanent in verandering. Dit geldt natuurlijk ook voor de fiscaliteit: de wet- en regelgeving en jurisprudentie inzake de loonheffingen verandert doorlopend.

Dit houdt in dat in het TCF moet worden geborgd dat HRM-medewerkers en salarisadministrateurs in voldoende mate en tijdig op de hoogte zijn van ontwikkelingen in de loonheffingen. Ook kan in het TCF worden geregeld dat bij de ontwikkeling van nieuwe arbeidsvoorwaarden een interne of externe loonheffingdeskundige is betrokken. De organisatie dient voortdurend de opzet, het bestaan en de werking van het TCF te bewaken. Interne en externe accountants en specialisten kunnen een rol spelen bij het evalueren en testen van een TCF. Zo zal de organisatie op een effectieve en efficiënte wijze invulling kunnen geven aan de interne risicobeheersings- en -controlemaatregelen voor de fiscaliteit.

Opgave 4.2

1. Salarisverwerking kan op de volgende wijzen plaatsvinden:
 - zelf zorg dragen voor de salarisverwerking (vereist een gekwalificeerde salarisadministrateur);
 - uitbesteden aan de accountant;
 - uitbesteden aan de softwareleverancier.

2. Als een onderneming niet wil dat bestanden in de cloud leesbaar zijn, kan men deze versleutelen voordat ze de cloud ingestuurd worden.
3. De medewerker hoeft bij SSO slechts één keer in te loggen. Hierdoor is er geen noodzaak meer allerlei gebruikersnamen en wachtwoorden te onthouden en deze op kladbriefjes te noteren, met de bijbehorende veiligheidsrisico's.
4. Deze vallen niet onder de definitie van datalek. Het gaat wel om derden die geen toegang zouden mogen hebben tot de gegevens, maar deze toch in handen krijgen. Maar het betreft geen persoonsgegevens.
5. Het doel van de AVG is het verzekeren van bescherming van de persoonsgegevens en het waarborgen van het vrije verkeer van persoonsgegevens binnen de EU. In de AVG wordt het recht van de betrokken persoon op hoog niveau beschermd.
6. Elke organisatie die personeel in dienst heeft, dus ook Concern nv, moet intern privacybeleid publiceren. Hierin staat wie welke rol heeft bij de omgang met persoonsgegevens. Het is belangrijk dat medewerkers hiervan op de hoogte zijn. Zij moeten dus worden getraind, en dit moet geregeld worden herhaald.
7. Horizontaal toezicht betekent samenwerking tussen Belastingdienst en ondernemingen. Doordat partijen die bij het aangifteproces betrokken zijn goede afspraken maken, wordt de kwaliteit van de aangiften behouden en verbeterd. Ook wordt onnodig dubbel werk voorkomen.
8. De Belastingdienst:
 - stemt de vorm en intensiteit van zijn toezicht af op de kwaliteit van de interne beheersing, interne controle en externe controle;
 - zorgt voor het tijdig uitbetalen van belastingteruggaven;
 - geeft zo snel mogelijk na ontvangst van een ingenomen of in te nemen standpunt en zo veel mogelijk in overleg met de ondernemer zijn visie op de rechtsgevolgen;
 - houdt bij het geven van zijn visie ten aanzien van de rechtsgevolgen rekening met relevante termijnen;
 - bespreekt de (fiscaal) relevante zaken, waarbij vanuit zijn optiek mogelijk verschil in inzicht kan ontstaan (periodiek) met de ondernemer;
 - licht toe en legt uit waarom hij bepaalde informatie vraagt aan de ondernemer, waarbij de termijn voor beantwoording in overleg wordt vastgesteld;
 - bevordert het werken in de actualiteit. De aanslagen worden zo spoedig mogelijk na de indiening van de aangifte en zo veel mogelijk in overleg met de ondernemer vastgesteld.
9. Concern nv moet een analyse of nulmeting doen op de fiscale processen, de fiscale techniek en de ICT-systemen. Zo ontstaat een beeld van waar aanvullende controlemaatregelen moeten worden getroffen.

Voor de loonheffingen betekent dit dat een goede analyse van de bestaande situatie moet worden gemaakt. In deze analyse moet de organisatie aandacht besteden aan:

 - salarisverwerking, zowel inhoudelijk als procesmatig;
 - beoordeling van de arbeidsvoorwaarden in het licht van een juiste verwerking van de loonheffingen;
 - verantwoordelijkheden m.b.t. een juiste verwerking van salariscomponenten;
 - beoordeling van de ICT-systemen.

10. In het kader van horizontaal toezicht kan het voor Concern nv verstandig zijn de opzet, het bestaan en de werking van het TCF te laten toetsen door de accountant. Een degelijke kwaliteitsstempel past volledig in het beeld van in control zijn, ook voor de loonheffingen.

Opgave 4.3

1. Toepassen door het management van e-HRM richting medewerkers (ter verbinding):
 - nieuws over personeel;
 - nieuws over afdelingen;
 - nieuws over de organisatie;
 - verjaardagen;
 - jubilea;
 - andere belangrijke momenten;
 - input vragen via polls of enquêtes.
2. Mogelijkheden van een ESS-systeem:
 - online toegang tot loonstrookjes;
 - naw-gegevens wijzigen;
 - belastingafhankelijke bedragen en aftrekbedragen wijzigen;
 - verzuim melden;
 - verlof boeken;
 - uren loggen;
 - keuzes aangeven binnen het cafetariasysteem;
 - wijzigingen aanbrenge in pensioeninvesteringsplannen, zoals het wijzigen van werknemersbijdragen;
 - opzetten van leningen;
 - opnemen van opnames;
 - onkostenbeheer, indienen van declaraties;
 - opgeven van zakelijk gereden kilometers.
3. Dat is een voorbeeld van single sign-on (SSO) oftewel eenmalig inloggen.
4. Gebeurtenissen die niet gemeld hoeven te worden aan de Autoriteit Persoonsgegevens:
 - Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden.
 - Iemand laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een deugdelijk slot, en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.
 - Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal vaak leiden tot het nodige ongemak voor vereniging en leden, maar zal niet snel aanleiding geven tot een melding bij de AP. Melding is meestal wel nodig als de sportvereniging zich bijvoorbeeld richt op personen met een specifieke levensovertuiging of seksuele geaardheid of als er fraudegevoelige gegevens gelect zijn.
 - Als ziekenhuispersoneel gebruikmaakt van het wachtwoord van een arts om toegang te krijgen tot medische persoonsgegevens, is dit geen datalek maar schending van interne voorschriften. Dan liggen disciplinaire maatregelen voor de hand.

5. Naast bestanden met namen, adressen en dergelijke, vallen nu ook andere gegevens onder de wet zoals IP-adressen, MAC-adressen en cookies.
6. Een functionaris voor de gegevensbescherming (FG), ook wel ‘privacy officer’, is een onafhankelijke persoon binnen de organisatie die adviseert en rapporteert over naleving van de AVG. Dit is verplicht wanneer de organisatie op grote schaal gevoelige persoonsgegevens zoals gezondheidsgegevens verwerkt, of als deze structureel mensen observeert (fysiek of digitaal). Een FG kan iemand zijn die intern aangesteld wordt, maar mag ook iemand zijn die extern aangesteld wordt, zoals een (virtuele) privacy officer.
7. Voordelen van samenwerking rond horizontaal toezicht:
 - één aanspreekpunt bij de Belastingdienst: hierdoor is een open en transparante communicatie voor alle betrokkenen beter mogelijk;
 - sneller zekerheid over de aanslag: horizontaal toezicht helpt de onderneming bij het tijdig signaleren en beheersen van fiscale risico's. Hierdoor is er sneller duidelijkheid over de fiscale positie, meer gemoedsrust en meer ruimte om te ondernemen;
 - aangepast toezicht, bijvoorbeeld bij controles en vragenbrieven: werken in het verleden maakt plaats voor werken in het heden. Door te kiezen voor horizontaal toezicht behoren boekencontroles tot de verleden tijd. Een belangrijke voorwaarde is dat de ondernemer op juiste en tijdige wijze aangifte doet. Mogelijke discussiepunten legt de onderneming vooraf aan de Belastingdienst voor en worden in samenspraak opgelost in plaats van door controle achteraf, waarbij de fiscus bij misstanden direct een boete oplegt.
8. Dit zijn koepelorganisaties voor administratiekantoren, accountants en boekhouders.
9. Bij horizontaal toezicht behoort sprake te zijn van:
 - a. transparantie: de ondernemer legt een in te nemen fiscaal standpunt zo snel mogelijk voor aan de Belastingdienst en de Belastingdienst geeft hierop in overleg zo snel mogelijk zijn visie op de rechtsgevolgen;
 - b. begrip: de Belastingdienst legt uit waarom hij bepaalde informatie aan de ondernemer vraagt en de ondernemer onderbouwt zijn reactie zo goed mogelijk;
 - c. wederzijds vertrouwen: de ondernemer wekt vertrouwen bij de Belastingdienst door open te zijn inzake fiscale vraagstukken en de Belastingdienst toont vertrouwen te hebben door het beperken van het aantal controles.
10. Melding van een datalek hoeft niet plaats te vinden als het onwaarschijnlijk is dat er risico's zijn voor de privacy van de betrokken personen. Maar dit datalek moet wel worden gelogd in het datalekkenregister van de verantwoordelijke organisatie, dus bij Primula bv. In dit register moeten alle datalekken namelijk worden opgenomen. Naast de informatie over het lek zelf en de genomen maatregelen moeten de overwegingen voor het wel of niet melden worden opgenomen. Als het datalek waarschijnlijk een hoog risico inhoudt, moet Primula bv ook de betrokkenen informeren.

Opgave 4.4

1. Mogelijkheden tot salarisverwerking bij samenwerking met een softwareleverancier:
 - salarisverwerking uitvoeren met behulp van allerlei online oplossingen;
 - salarisverwerking volledig uitbesteden: van personeelsadministratie tot uitbetaling;
 - tussenoplossing, waarbij de softwareleverancier zorgt dat de salarisverwerking in orde is, de juiste wet- en regelgeving is toegepast en er een correcte loonspecificatie is.
2. Een frauderende medewerker kan door het wijzigen van zijn huisadres in een veel verder weg gelegen fictief woonadres onterecht periodiek een veel te hoge onbelaste reiskostenvergoeding ontvangen. Er moeten maatregelen worden genomen om dit te voorkomen.
3. Als iemand de informatie weet van de primaire login van een medewerker die met SSO werkt, kan hij inloggen op alle systemen waartoe die medewerker recht heeft.
4. Encryptie is een goede manier om privacygevoelige informatie te versturen of op te slaan in de cloud. Mocht er een datalek optreden, dan is de informatie nog steeds veilig.
5. Elswoud Elektrotechniek moet alle datalekken intern documenteren, ook datalekken die niet aan de Autoriteit Persoonsgegevens gemeld hoeven te worden.
6. Verouderde gegevens moeten op verzoek worden gewist. Een verzoek van een betrokkene (bijvoorbeeld een personeelslid) over zijn persoonsgegevens moet binnen een maand inhoudelijk afgehandeld zijn.
7. De twee hoofdgroepen bij horizontaal toezicht zijn:
 - grote ondernemingen;
 - het midden- en kleinbedrijf.
8. Acco als fiscaal dienstverlener verklaart zich bereid op een open en transparante manier met de Belastingdienst samen te werken, bijvoorbeeld door fiscale kwesties vooraf te bespreken. De fiscaal dienstverlener staat in voor de kwaliteit van de ingediende aangiften.
9. De uiteindelijke verantwoordelijkheid voor een TCF ligt bij de leiding van de organisatie. Voor de inrichting van het TCF is het echter van groot belang om in kaart te brengen hoe de verantwoordelijkheden van de fiscale functie zijn verdeeld. Dikwijls blijkt dat deze verdeling van verantwoordelijkheden niet eenvoudig is vast te stellen. Voor de loonheffingen kan bijvoorbeeld de vraag opkomen wie nu de echte verantwoordelijke is voor de juiste, volledige en tijdige aangifte. Is dat de afdeling HRM, salarisadministratie of financiële administratie?
Een andere vraag betreft de verantwoordelijkheid voor het werken met zelfstandigen die niet in de salarisadministratie voorkomen. De onderneming moet zich bij dit soort vragen realiseren dat tal van medewerkers direct of indirect betrokken zijn bij de fiscale functie. Veel van deze medewerkers rapporteren functioneel of organisatorisch niet direct aan de verantwoordelijke voor de loonaangifte. Zo heeft het hoofd van wagenparkbeheer een belangrijke rol bij de communicatie naar de afdeling salarisadministratie als het gaat om de juiste cataloguswaarde van de leaseauto's die de medewerkers gebruiken. De organisatie moet absoluut de veelheid van rollen en verantwoordelijkheden in kaart brengen, die van invloed kunnen zijn op de juiste verwerking van de loonheffingen.

Opgave 4.5

1. Salarisverwerking kan in de cloud via software as service (SaaS). De onderneming is zelf verantwoordelijk voor de salarisverwerking, maar regelt dit via een online dienst. Daardoor hoeft er geen dure, eventueel maatwerksoftware aangeschaft te worden, maar werkt de onderneming op aanwijzingen van de clouddienstverlener. (De meeste leveranciers van salarispakketten bieden de keuze tussen het kopen van software die bij de onderneming zelf wordt geïnstalleerd en het werken in de cloud met software bij de leverancier).
2. Relevante vragen bij de keuze voor een salarisverwerker:
 - Ondersteunt de salarisverwerker geautomatiseerde regelingen zodat wij deze niet met de hand hoeven te verwerken? Bijvoorbeeld WW-premies, zorgverzekeringen, kilometervergoedingen, overwerk, verlof en uitruilmogelijkheden van salariscomponenten.
 - Hebben wij de mogelijkheid om de definitieve berekening vooraf te controleren?
 - Zijn controle-, pro-forma berekeningen en correcties inclusief én zonder additionele kosten?
 - Kunnen wij zelf overzichten maken? Of zijn wij tegen meerkosten afhankelijk van de salarisverwerker?
 - Kunnen wij gegevens eenvoudig exporteren en importeren? Bijvoorbeeld mutaties uit ons urensysteem, gegevens voor rapportages en uitwisselen van gegevens met andere applicaties.
 - Kunnen wij onze eigen regelingen kwijt in het systeem?
 - Kunnen wij zelf aanpassingen doorvoeren? Of zijn wij afhankelijk van de leverancier en krijgen wij de rekening?
 - Hebben wij ruimte een eigen interpretatie te geven aan de standaardregelingen? Of zijn wij afhankelijk van de gekozen inrichting van de salarisverwerker?
 - Geven wij de voorkeur aan een standaardinrichting en dienstverleningspakket of willen wij liever een op maat ingericht systeem met bijbehorende dienstverlening? Biedt de toekomstige salarisverwerker deze mogelijkheden?
 - Biedt de salarisverwerker meer dan alleen een loonstrook? Wat is onze HR-ambitie? Kan de leverancier deze invullen?
 - Kunnen wij de zelfredzaamheid van teamleiders en medewerkers vergroten door gebruik van selfservicemogelijkheden?
 - Niet elk systeem ondersteunt meerdere dienstverbanden. Hoe belangrijk is dit voor onze organisatie?
 - Kunnen wij aanvragen, mutaties en declaraties altijd en overal indienen of zitten wij vast aan bepaalde tijden?
 - Is de toekomstige leverancier ISAE3402 Type II-gecertificeerd?
 - Is informatie real-time beschikbaar of is er sprake van vertraging doordat bepaalde informatie nog niet is bijgewerkt of moet worden ingelezen?
 - Biedt onze toekomstige leverancier de flexibiliteit om delen van het salarisproces uit te besteden en de mate van uitbesteding aan te passen naar behoefte in de tijd?
 - Krijgen wij één vast contactpersoon, met back-up, die op de hoogte is van de wet- en regelgeving, onze organisatie, de medewerkers en de software?

- Zitten wij vast aan een langdurig contract of is er de mogelijkheid tussentijds te switchen? Bijvoorbeeld meer of minder taken zelf doen, extra controlewerkzaamheden.
3. Bij authenticatiemanagement wordt het loginproces vereenvoudigd door gebruik te maken van de combinatie pincode met gebruikerspas. De gebruiker 'swipet' bij het inloggen zijn gebruikerspas langs een lezer en vult alleen een pincode in. Daarna is de gebruiker ingelogd op zijn werkstation en kan hij vervolgens alle applicaties openen die hij nodig heeft, zonder nogmaals in te loggen. Hier is dus sprake van two factor authentication (tweefactorautorisatie).
 4. Encryptie is het coderen (versleutelen) van gegevens door middel van een bepaald algoritme. Alleen de partijen met de juiste sleutel, kunnen de gegevens weer decoderen. Zonder sleutel is de data waardeloos.
 5. Een datalek moet gemeld worden aan de Autoriteit Persoonsgegevens.
 6. De 100%-filosofie houdt in dat de belastingplichtige wettelijk verplicht is aangifte te doen, de inspecteur toetst vervolgens of de aangifte voldoet aan wet- en regelgeving en corrigeert als er afwijkingen zijn van de wet. Door middel van straffen en boetes wordt de burger afgeschrikt om de regels te overtreden. Deze vorm van handhaving gebeurt louter achteraf.
 7. Met een convenant willen beide partijen komen tot een effectieve en efficiënte werkwijze. Zij streven naar permanent actueel inzicht in de relevante gebeurtenissen en snelle standpuntbepaling om zo de rechtszekerheid te vergroten.
 8. Voor samenwerking met de brancheorganisaties zijn er twee mogelijkheden:
 - Als een branche zelf een eigen vorm van toezicht binnen de branche heeft, kan dat leiden tot het afsluiten van een horizontaaltoezichtconvenant.
 - Is er geen eigen vorm van toezicht bij de brancheorganisatie, dan kunnen met de Belastingdienst wel brancheafspraken over fiscale zaken worden gemaakt. Afspraken over toezicht worden dan niet opgenomen in het convenant. Er is in dat geval sprake van een overlegplatform. Een voorbeeld hiervan is het convenant dat is afgesloten met de sector Binnenvaart.
 9. Het is van belang dat de organisatie alle processen vastlegt die op enige wijze van invloed kunnen zijn op de juiste verwerking van de loonheffingen. In de praktijk blijkt dat zo'n 80% van deze vastlegging wel plaatsvindt. De onderneming moet al deze voor de loonheffingen relevante gegevens verzamelen en waar nodig aanscherpen. De overige (ook belangrijke) processen moet de organisatie nader ontwerpen en uitschrijven, bijvoorbeeld via stroomschema's met toelichtingen. Zo kan de onderneming een stroomschema maken om de risico's te beheersen van betalingen aan medewerkers die niet in loondienst zijn. In deze beheersmaatregel worden de stappen in het proces benoemd, samen met de risico's en de controle en monitoring. Uiteraard zal deze vastlegging per werkgever verschillen en kunnen de documenten worden aangevuld met een toelichting.

Opgave 4.6

1. Het is van belang de technische infrastructuur en de organisatie van de ICT-afdeling te beoordelen om vast te stellen of betrouwbare gegevensverwerking mogelijk is. Vindt er een juiste en volledige overdracht van gegevens plaats tussen het HRM-systeem en het daaraan gekoppelde salarisverwerkingsysteem? Ook moet gedacht worden aan de beoordeling van de ICT-controls: wie heeft toegang tot welke onderdelen van het HRM- en salarissysteem (bijvoorbeeld vanuit beveiliging en controletechnische functiescheiding)? Overigens is hier niet van belang of de daadwerkelijke salarisverwerking is ondergebracht bij een externe partij. Ook als de salarisverwerking plaatsvindt bij een extern bedrijf, blijft de werkgever fiscaal verantwoordelijk voor de juiste verwerking van de salarissen.
2. ‘Agree to disagree’ houdt in dat de Belastingdienst en de onderneming bij horizontaal toezicht van mening kunnen verschillen. Ze zijn het er tijdens het vooroverleg over eens dat ze het niet met elkaar eens hoeven te zijn. Dit betekent dat de onderneming een aangifte kan indienen die afwijkt van de visie van de Belastingdienst. Of de onderneming dient een aangifte in die overeenstemt met de Belastingdienst. In beide gevallen staat de bezwaar- en beroepsprocedure open.
Belangrijk is dat beide partijen vanaf de aanvang door de transparantie (openheid van zaken) weten dat ze een verschil van inzicht hebben. Boetes zijn in deze situatie niet aan de orde.
3. Op grond van de Algemene wet bestuursrecht (AWB) wordt onder toezicht verstaan: het bij of krachtens wettelijk voorschrift belast zijn met het houden van toezicht op de naleving van wat bij of krachtens enig wettelijk voorschrift is bepaald.
4. De maximale boete per overtreding van de Wbp was € 900.000. Dit bedrag is met de komst van de AVG verhoogd naar € 20 miljoen of 4% van de wereldwijde jaaromzet.
5. Deze convenanten zijn gebaseerd op transparantie, begrip en wederzijds vertrouwen. Daarbij is het uitgangspunt dat er voldoende aandacht is voor de fiscale beheersing binnen de onderneming (tax control framework, TCF). Voor deze convenanten heeft de Belastingdienst een standaardtekst gemaakt.
6. Dit zwakke punt van SSO kan worden opgelost met 2FA (tweefactorautorisatie).
7. Afspraken die de Belastingdienst in het kader van horizontaal toezicht maakt met een fiscaal dienstverlener die aan de voorwaarden voldoet:
 - De samenwerking vindt plaats op basis van vertrouwen, begrip en transparantie.
 - De wet- en regelgeving blijft onverkort van toepassing.
 - De koepelorganisaties staan in voor de kwaliteit van de deelnemende fiscaal dienstverleners, bijvoorbeeld door een kwaliteitssysteem te hanteren en reviews te houden.
 - De Belastingdienst past zijn werkwijze aan (contactpersoon, vooroverleg en toezicht).
8. We spreken hier van ESS (Employee Self Service) en van MSS (Manager Self Service); beide zijn onderdeel van een uitgebreid e-HRM-pakket.
9. Er zijn omstandigheden mogelijk die leiden tot beëindiging van het horizontaal toezicht met Vast Goed. Het uitgangspunt is dat de Belastingdienst deelname alleen onder zwaarwegende omstandigheden opzegt. De Belastingdienst geeft de redenen door aan de onderneming en uiteraard bestaat eerst nog de mogelijkheid tot overleg.

Juist of onjuist?**Opgave 4.7**

Onjuist. Handmatige salarisverwerking is toegestaan, alleen de loonaangifte moet digitaal.

Opgave 4.8

Juist.

Opgave 4.9

Onjuist. De gebruiker is geen eigenaar van de gebruikte hard- en software en is dus ook niet verantwoordelijk voor het onderhoud. De onderneming zelf heeft alleen nog terminals nodig om te werken. De rest van de hardware en software bevindt zich bij de provider.

Opgave 4.10

Juist.

Opgave 4.11

Juist.

Opgave 4.12

Juist.

Opgave 4.13

Onjuist. Cloud computing is het via een netwerk (online) op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet.

Opgave 4.14

Onjuist. De medewerker kan bepaalde gegevens wel wijzigen, zoals bijvoorbeeld een woonadres, een aanvraag voor verlofdagen, een keuze binnen het cafetariasysteem enzovoort.

Opgave 4.15

Onjuist. De gebruiker hoeft zich slechts één keer aan te melden en dat doet de medewerker met de gebruikelijke aanmeldprocedure op de computer.

Opgave 4.16

Onjuist. Hier is geen sprake van een datalek, maar van schending van interne voorschriften. Dan ligt het nemen van disciplinaire maatregelen voor de hand.

Opgave 4.17

Onjuist. Externe dienstverlener neemt salarisverwerking over op locatie van opdrachtgever.

Opgave 4.18

Juist.

Meerkeuzevragen

Opgave 4.19

Nadelen van een geïntegreerd HRM-systeem:

- c. bij upgrades van het systeem gaat maatwerk vaak verloren;
- e. minder geschikt voor specifieke, complexe processen binnen bedrijf zoals bijvoorbeeld tijdsregistratie;
- f. overstappen moeilijk wegens de gedane investeringen;
- g. soms minder maatwerkmogelijkheden;
- h. vaak minder flexibel.
- i. aan nieuwe HRM-behoefte in de toekomst kan het geïntegreerde systeem slechts in beperkte mate of pas na verloop van tijd voldoen.

Opgave 4.20

- b. Stelling I is juist en stelling II is onjuist.

Opgave 4.21

De volgende maatregelen:

- a. functiescheiding;
- b. invoercontrole op juistheid;
- c. softwaremaatregelen, bijvoorbeeld het up to date houden van de browser;
- d. hardwaremaatregelen, bijvoorbeeld gebruikmaken van biometrische herkenning via vingerafdruk of irisscan;
- e. fysieke maatregelen, bijvoorbeeld het afsluiten van USB-poorten;
- f. gebruikersmaatregelen, bijvoorbeeld het werken met wachtwoorden en goede instructies.

Opgave 4.22

Voordelen van single sign-on zijn:

- a. betere beveiliging van het netwerk;
- c. de eindgebruiker is productiever;
- d. eenvoud voor de eindgebruiker;
- e. minder wachtwoord reset aanvragen bij de afdeling ICT.

Opgave 4.23

De AVG legt in het kader van persoonlijke gegevens de volgende verplichtingen op aan organisaties:

- a. een organisatie moet alle verwerkingen van persoonlijke gegevens documenteren, ook de alledaagse zoals de personeelsadministratie of een nieuwsbrief;
- c. de beveiliging moet op orde zijn, en op orde blijven;
- e. in eenvoudige taal moet een organisatie precies en volledig uitleggen wat deze doet met persoonlijke gegevens. Ook moet men mensen wijzen op hun rechten en er bijvoorbeeld op wijzen dat men gegevens mag (laten) aanpassen, het dossier mag inzien of zelfs laten vernietigen.

Opgave 4.24

Aan verticaal toezicht zijn de volgende nadelen verbonden:

- a. boekenonderzoeken bij belastingplichtigen zijn erg tijdrovend;
- b. de Belastingdienst vraagt informatie op en de belastingplichtige is verplicht deze aan te leveren. Daardoor ontstaat er een relatie tussen beide partijen die in het teken staan van wantrouwen en confrontatie;
- c. het toezicht gaat gepaard met weinig vertrouwen tussen de Belastingdienst en de belastingplichtige. Dit kan ertoe leiden dat de beide partijen niet alle relevante informatie met elkaar delen. Hierdoor kunnen geschillen onnodig lang duren wat hoge kosten met zich brengt. Deze vorm gaat gepaard met een duidelijke hiërarchische verhouding;
- e. de Belastingdienst moet voldoende capaciteit en voldoende controledichtheid hebben om goede handhaving te kunnen bewerkstelligen.

Opgave 4.25

Horizontaal toezicht door de Belastingdienst kan van toepassing zijn op de:

- a. dividendbelasting;
- b. inkomstenbelasting;
- c. loonbelasting;
- d. omzetbelasting;
- f. vennootschapsbelasting.

Opgave 4.26

Bij horizontaal toezicht kan de Belastingdienst samenwerkingsafspraken maken met:

- a. brancheorganisaties;
- b. fiscaal dienstverleners;
- c. grote ondernemingen;
- e. koepelorganisaties van fiscaal dienstverleners.

Opgave 4.27

Voorbeelden van soft controls zijn:

- b. houding van de leiding;
- c. integriteit;
- e. waarden en normen.

Opgave 4.28

Een werkgever moet ten aanzien van personeel in een tax control framework de volgende processen opnemen:

- a. in dienst nemen van werknemers;
- b. de arbeidsvoorwaarden en aanpassingen daarvan;
- c. beëindigen van dienstbetrekkingen;
- d. alle vormen van declaraties, inclusief vaste kostenvergoedingen;
- e. inhuren van arbeidskrachten voor wie geen loonheffingen worden ingehouden;
- f. registratie van tijd.

Opgave 4.29

Voorwaarden voor deelname aan horizontaal toezicht door de Belastingdienst:

- a. de taken, verantwoordelijkheden en bevoegdheden van elke functie zijn helder beschreven;
- b. er is een intern controleplan met een ideale controlemix en periodieke audits;
- d. er is een risicoanalyse opgesteld waarin beheersmaatregelen staan om 'in control' te zijn en te blijven.

Opgave 4.30

Voorwaarden voor horizontaal toezicht voor een onderneming:

- a. de taken, verantwoordelijkheden en bevoegdheden van elke functie moeten helder beschreven zijn;
- b. de administratieve organisatie en interne controle (aoic) moeten goed op orde zijn;
- d. er moet een risicoanalyse zijn opgesteld, waarna beheersmaatregelen worden vastgelegd;
- e. er moet een beheersmodel worden ingericht, waarna uit rapportages de opzet, het bestaan en de werking van beheersmaatregelen blijkt.

Opgave 4.31

Authenticatiefactoren bij toepassing van 2FA zijn:

- b. een mobiele telefoon, speciale usb-key of gebruikerspas;
- d. een vingerafdruk of andere biometrische eigenschap;
- e. een wachtwoord of pincode.

Opgave 4.32

Voorbeelden van een datalek zijn:

- b. de servers van een bedrijf worden gehackt en er wordt gevoelige klantinformatie gestolen;
- c. een geprinte lijst met klantgegevens wordt gestolen;
- d. een medewerker verliest een smartphone, laptop of usb-stick met gevoelige persoonsinformatie.

Opgave 4.33

Hier is sprake van:

- b. prestatieloon;
- d. stukloon.

Opgave 4.34

- a. Stelling I en II zijn beide juist.

Casussen**Opgave 4.35**

Beveiligingsmaatregelen voor het geautomatiseerde kantoor				
	software- maatregel	hardware- maatregel	fysieke maatregel	gebruikers- maatregel
Het afsluiten van de USB-poorten			x	
Het gebruikmaken van biometrische herkenning via vingerafdruk of irisscan		x		
Het up-to-date houden van de browser	x			
Het werken met wachtwoorden en goede instructies				x

Opgave 4.36

Melding aan Autoriteit Persoonsgegevens ...		
	verplicht	niet verplicht
Door een haperende beveiliging zijn medische gegevens ingezien door onbevoegden.	x	
Een brief met daarin persoonsgegevens wordt ongeopend teruggestuurd.		x
Een goed afgesloten koffer met daarin persoonsgegevens wordt in de trein achtergelaten en weer terugbezorgd bij de eigenaar.		x
Een medewerker van een internetprovider geeft zijn logingegevens aan een derde partij gegeven die daardoor bij alle klantgegevens kan komen.	x	
Een personeelslid verliest een laptop met financiële klantgegevens.	x	
Van een muziekvereniging wordt de ledenadministratie gehackt.		x

Opgave 4.37

	verticaal toezicht	horizontaal toezicht
Belastingdienst maakt afspraken met partijen die betrokken zijn bij de aangifte		x
Belastingdienst vraagt info op en belastingplichtige moet leveren	x	
Belastingdienst biedt vooraf zekerheid over fiscale kwesties		x
Ondernemer moet in control zijn		x
Er is sprake van samenwerking tussen fiscus en belastingplichtige		x
Er is sprake van tijdrovende boekenonderzoeken	x	
Relatie staat in het teken van wantrouwen en confrontatie	x	

Opgave 4.38

- a. P&O hoeft niet meer na te bellen als er stukken ontbreken of incompleet zijn. Vroeger moesten werknemers die een declaratie wilden indienen eerst op zoek naar het juiste formulier, dit vervolgens volledig invullen – inclusief gegevens die al lang bekend waren bij de organisatie – en de aanvraag in het postvakje van hun manager leggen. De leidinggevende moest de aanvraag ondertekenen, deze naar de HR-afdeling doorsturen, die het weer naar de salarisadministratie zond. Tijdens dit proces kon veel fout gaan. Nu voert de medewerker de juiste gegevens zelf in. Na controle en accordering kan betaald worden.
- b. Nu zijn alle procedures vastgelegd in e-HRM. Dit houdt in dat alle belangrijke data automatisch bewaakt worden. Het systeem genereert zelf een verzoek en eventueel een herinnering aan de lijnmanager, zodat deze op de hoogte is. De tijdigheid is nu veel beter. De HR-afdeling hoeft geen tijd te steken in bewaken, rappelleren, nabellen en dergelijke.
- c. Tegenwoordig worden bijvoorbeeld verlofaanvragen door medewerkers zelf ingevoerd in e-HRM. De datum of periode staat direct in het systeem, in plaats van na een arbeidsintensieve papieren procedure. Soms kan het systeem zelf akkoord geven, in andere gevallen doet de leidinggevende dat. De roosterplanner beschikt steeds over de meest actuele gegevens. Correcte werkroosters zijn mogelijk en het aantal correcties is veel beperkter.
- d. Nu voert de werknemer de declaratie zelf in. Een datumveld moet verplicht ingevuld worden, zodat deze niet ontbreekt. Dat geldt ook voor de andere benodigde informatie. De beoordelaar van de declaratie heeft snel inzicht en kan direct accorderen. In de meeste gevallen zal het niet nodig zijn om nog fouten te corrigeren.
- e. Alle gegevens worden slechts eenmaal ingevoerd en vervolgens gecontroleerd. Iedere betrokkene binnen Hulst bv gebruikt dezelfde basisgegevens. Veel dubbel invoerwerk wordt voorkomen.
- f. Elk gegeven wordt slechts één keer ingevoerd in e-HRM. Het systeem biedt voor alle betrokkenen de gewenste rapportagemogelijkheden. Elke afdeling heeft daardoor een optimaal overzicht van de relevante informatie.