Whistleblower-system – en konflikt mellan amerikanska SOX och den svenska personuppgiftslagen

av Henrik Bengtsson och Johan Kahn

Den svenska Datainspektionen har den 26 mars 2008 meddelat beslut i fem ärenden avseende undantag från 21 § personuppgiftslagen beträffande s k whistleblower-system.[1] Datainspektionen har en restriktiv syn på hur whistleblower-system får vara utformade. Det innebär att många amerikanska och svenska företag i praktiken kommer att hamna i en konflikt mellan amerikanska Sarbanes Oxley Act (SOX) och personuppgiftslagen.

SOX och whistleblowersystem

Efter de ökända amerikanska Enron- och Worldcomskandalerna tillkom SOX. Lagen reglerar hur bolag som är noterade på amerikanska börser skall styras. SOX innebär bl a att företagen skall ha ett s k whistleblower-system. Genom ett whistleblower-system är det meningen att anställda anonymt skall kunna rapportera oegentligheter som till exempelvis ekonomisk brottslighet, uppblåsta siffror eller etiska överträdelser till en s k audit committee. På så sätt kan företaget på ett tidigt stadium utreda och förhindra brottslig verksamhet, skador och dålig publicitet.

I artikel 301 (4) SOX regleras skyldigheten att införa whistleblower-system:

> *[Each audit committee shall] «establish procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters».*

New York-börsens (NYSE) och Nasdaqs regelverk innehåller motsvarande skyldigheter. SOX innehåller inga regler som begränsar lagens territoriella räckvidd. Amerikansk rättspraxis rörande SOX extraterritoriella räckvidd är splittrad[2] men många företag utgår från att lagen även kommer att tillämpas på europeiska dotterbolag. Eftersom NYSE och Nasdaqs regelverk träffar alla utländska företag vars aktier handlas på dessa börser får reglerna stor räckvidd i praktiken.

Artikel 301(4) innebär inget formkrav avseende utformningen av whistleblower-system[3]. Ett whistleblower-system kan exempelvis bestå i telefonbaserade eller webbaserade gränssnitt. Många företag har dock valt att inrätta whistleblower-system där anställda via ett webbgränssnitt kan rapportera misstänkta brott och oegentligheter inom bolaget till bolagets redovisningskommitté i USA.

Datainspektionens beslut

Eftersom behandling av personuppgifter om misstänkta lagöverträdelser inte är tillåten enligt 21 § PUL har ett antal svenska dotterbolag till amerikanska bolag som lyder under SOX- och börsreglerna ansökt om undantag från förbudet mot behandling av lagöverträdelser enligt 21 § PUL hos Datainspektionen. Datainspektionen har samtidigt fattat beslut i ärendena och besluten innebär i korthet att förutsätt ningarna för att behandling av uppgifter inom ett whistleblower-system är att:

1. Systemet ska utgöra ett komplement till normal internförvaltning och måste vara frivilligt att använda. Systemet får bara användas när det är sakligt motiverat att inte använda företagets interna informations- och rapporteringskanaler.

2. Systemet för whistleblowing ska begränsas till allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor samt brottslighet inom bank- och finansväsen. Det kan även avse andra allvarliga oegentligheter som rör företagets vitala intressen eller enskildas liv och hälsa.
3. Endast anställda i nyckelpositioner eller ledande ställning får anmälas och behandlas i systemet.
4. Den personuppgiftsansvarige måste se till att bestämmelserna i personuppgiftslagen följs för den del av behandlingen som bolaget ansvarar för, t.ex. när det gäller känsliga personuppgifter, information till de anställda och överföring av personuppgifter till tredje land.

Datainspektionens skäl för att begränsa besluten till personer i ledande ställning är att ett whistleblower-system endast bör användas när det är sakligt motiverat att inte använda de normala interna informationskanalerna.

I tillägg till besluten ovan bör även nämnas att de grundläggande reglerna för personuppgiftsbehandling (9 § PUL) som innebär att personuppgiftsbehandling måste vara i överensstämmelse med god sed på svensk arbetsmarknad. I ett samrådsyttrande från Datainspektionen (Dnr 177-2006) konstateras att det saknas underlag i samrådsbegäran för att utreda frågan fullständigt. Datainspektionen hänvisar dock till Artikel 29-gruppens[4] uttalanden och understryker vikten av att whistleblower-systemet utformas i enlighet med de grundläggande reglerna för personuppgiftsbehandling. Det kan även antas att det enligt lagen om medbestämmande i arbetslivet föreligger en förhandlingsskyldighet i förhållande till aktuella arbetstagarorganisationer innan ett whistleblower-system införs.

PULs tillämplighet på webbaserade whistleblower-system

Huvudprincipen i 4 § PUL är att lagen är tillämplig på personuppgiftsansvariga som är etablerade i Sverige. I ovan nämnda beslut har Datainspektionen gjort en extensiv tolkning av personuppgiftsansvarsbegreppet och ansett att ett svenskt dotterbolag är personuppgiftsansvarigt för insamling och utlämnande av personuppgifter om dotterbolaget bereder svenska anställda möjlighet att använda ett whistleblower-system som det utländska moderbolaget tillhandahåller. Datainspektionen resonerar inte närmare kring på vilket sätt det svenska dotterbolaget i praktiken skulle ha faktisk och rättslig bestämmanderätt över behandlingen. Eftersom det i de behandlade ärendena är det amerikanska moderbolaget som ansvarar för whistleblower-systemet och vidtar åtgärder efter att ha mottagit anmälningar i systemen menar vi att det är det amerikanska moderbolaget som är personuppgiftsansvarig. Whistleblower-system implementeras oftast globalt och svenska dotterbolag har normalt endast förelagts att införa systemet av moderbolaget och har därför inte kontroll över utformningen av systemet. Frågan är om inte relationen mellan det amerikanska moderbolaget och det svenska dotterbolag enligt systematiken i PUL istället är att betrakta som den mellan personuppgiftsansvarig och -biträde och att tillämpligheten av PUL kan ifrågasättas på den grunden. Datainspektionens tolkning av personuppgiftsansvar får långtgående konsekvenser och man kan fråga sig om det skall tolkas på så vis att så snart arbetsgivaren ger en anställd tillgång till en databas i vilken användaren kan göra annat än bara ta del av uppgifter, i Sverige eller annars, blir arbetsgivaren personuppgiftsansvarig för behandlingen.

Synen på whistleblower-system inom EU

Frågan huruvida whistleblower-system är förenliga med dataskyddsdirektivet har varit omdebatterad i Europa. Den franska dataskyddsmyndigheten CNIL förbjöd 2005 McDonald's Corporation och Exide Technologies att tillhandahålla whistleblower-system utformade på visst sätt.[5] Efter de franska besluten inleddes samtal mellan Artikel 29-gruppen och amerikanska Securities Exchange Commission[6] vilka resulterade i Artikel-29 gruppens Yttrande om tillämpningen av EU:s regler om uppgiftsskydd på interna system för uppgiftslämnande inom bokföring, intern bokföringskontroll, revision, bekämpande av mutor samt brottslighet inom bank- och finansväsen).[7] De nationella dataskyddsmyndigheterna i Belgien[8], Danmark[9], Frankrike[10], Nederländerna[11], och Tyskland[12] har också meddelat beslut eller utarbetat riktlinjer rörande whistleblower-system.

Artikel 29-gruppens riktlinjer innebär att frågan huruvida ett whistleblower-system är förenligt med dataskyddsdirektivet skall prövas mot bakgrund av följande punkter:[13]

i) Begränsning av vilka som kan rapportera i ett whistleblower-system. Detta gäller särskilt mot bakgrund av att endast allvarligare anklagelser bör vara föremål för rapportering
ii) Begränsning av vilka som kan bli rapporterade genom ett whistleblower-system. Artikel 29-gruppen menar att det företag som inför ett system för uppgiftslämnande noggrant bör bedöma om det kan vara lämpligt att begränsa antalet personer som kan rapporteras genom systemet, särskilt mot bakgrund av allvaret i de påstådda förseelser som rapporteras. De angivna personalkategorierna kan ibland omfatta samtliga anställda.

iii) Uppmuntrande av icke-anonym men konfidentiell rapportering i motsats till anonym rapportering. Skälen för detta ställningstagande är ibland annat de spekulationer som följer anonym rapportering samt svårigheter med att utreda en anklagelse om det inte finns möjlighet att ställa kompletterande frågor.
iv) Proportionalitet och riktighet hos den data som behandlas inom ramen för ett whistleblower-system.
v) Reglerna om lagring av personuppgifter måste efterlevas.
vi) Den personuppgiftsansvarige måste informera de registrerade om systemets existens, syfte och funktion, om mottagarna av rapporterna och om de rapporterade personernas rätt till tillgång, rättelse och radering av uppgifter.
vii) Den personuppgiftsansvarige måste vidta alla rimliga tekniska och organisatoriska försiktighetsåtgärder för att skydda uppgifterna när de samlas in, sprids och lagras.
viii) Om det företag som ansvarar för whistleblower-systemet är etablerat i USA skall företaget

1. vara anslutet till «safe harbor»-systemet eller
2. ha träffat avtal med dotterbolaget enligt klausuler i standardavtal som utfärdats av Kommissionen eller
3. tillämpa regler («binding corporate rules») som godkänts av en nationell dataskyddsmyndighet.

Ovan nämnda nationella riktlinjer och beslut ansluter nära till Artikel 29-gruppens riktlinjer. När det gäller frågan om vilka anställda som kan omfattas av ett whistleblower-system har de nationella dataskyddsmyndigheterna nära anslutit sig till punkten ii) ovan vilket innebär att den personuppgiftsansvarige skall göra en proportionalitetsbedömning huruvida samtliga anställda skall omfattas av systemet.

Synpunkter på Datainspektionens beslut och behovet av en ändring av 21 § PUL

Jämför man den svenska Datainspektionens hållning i frågan med de principer som tillämpas av dess nationella europeiska dataskyddsmyndigheterna kan man konstatera att Datainspektionen gjort en strängare proportionalitetsbedömning än sina europeiska motsvarigheter genom att Datainspektionen beslutat att ett whistleblower-system måste vara begränsat till överträdelser begångna av personer i ledande ställning. Datainspektionen gör också en mer strikt bedömning än Artikel 29-gruppen som i sina riktlinjer har uttalat följande beträffande begränsningen av vilka personer som omfattas av ett whistleblower-system:

> *«Med tillämpning av proportionalitetsprincipen rekommenderar arbetsgruppen att det företag som är ansvarigt för systemet för uppgiftslämnande noggrant bör bedöma om det är lämpligt att begränsa det antal personer som skall ha rätt att rapportera påstådda oegentligheter genom systemet för uppgiftslämnande, främst mot bakgrund av allvaret i de påstådda förseelser som rapporteras. Arbetsgruppen medger dock att de angivna personalkategorierna ibland omfattar samtliga anställda på vissa av de områden som täcks av detta yttrande.»*

Mot bakgrund av den sista meningen i Artikel 29-gruppens ovan citerade uttalande är det förvånande att Datainspektionen reservationslöst, och med samma formulering trots skilda omständigheter i samtliga fem beslut, begränsar besluten på så vis att uppgifter enbart får lämnas beträffande personer i ledande ställning. Det faktum att Datainspektion gör samma bedömning trots skilda omständigheter ger intrycket att Datainspektionen närmast etablerar en generell princip snarare än att göra en prövning av varje enskilt fall.

Av 21 § personuppgiftslagen följer att behandling av lagöverträdelser inte är tillåten. Datainspektionen och svenska domstolar[14] tillämpar en strikt tolkning av begreppet «lagöverträdelse» vilket innebär att även uppgifter som inte är konkretiserade att avse ett visst brott betraktas som lagöverträdelser. Enligt 21 § PUL har rätten att fatta beslut om undantag från 21 § PUL delegerats till Datainspektionen som under senare tid har bedömt ett flertal ärenden beträffande behandling av uppgifter av lagöverträdelser, bl a beträffande: vaktbolags fotografering av gripna klottrare (Dnr 366-2006), övervakning av återvinningsstationer med s k sopspioner (Dnr 750-2006), utredning av upphovsrättsintrång (Dnr 1631 och 1632-2006), privata utredningar avseende stulna försäkrade föremål (886-2007), utredning av bedrägeriförsök mot banker (Dnr 1402-2007) och utredning av spelfusk avseende Internetspel (Dnr 424-2007).

Datainspektionen har genom 1 § DIFS 1998:3 undantagit vissa behandlingar från 21 § PUL, exempelvis får personuppgifter om lagöverträdelser behandlas om behandlingen avser endast enstaka uppgift som är nödvändig för att rättsliga anspråk skall kunna fastställas, i ett enskilt fall eller om behandlingen avser endast enstaka uppgift som är nödvändig för att anmälningsskyldighet enligt lag skall kunna fullgöras. Några allmänna råd för förutsättningarna för undantag har dock inte publicerats utan tills vidare får principerna för undantag utläsas ur Datainspektionens onyanserade beslut. När det gäller behandling av personuppgifter i syfte att komma till rätta med överträdelser av de immaterialrättsliga lagarna har re-

geringen däremot föreslagit att ett undantag från 21 § PUL införs i dessa lagar.[15]

Det finns åtminstone en teoretisk möjlighet att straff skulle kunna utdömas i enlighet med 49 § PUL. Det är otillfredsställande att det inte direkt i lagen eller i vart fall i en förordning anges under vilka förutsättningar undantag från 21 § PUL. En myndighet som mycket väl kan bli part i mål om överklagade beslut att inte medge undantag bör inte ges uppgiften att genom ad hoc praxis utarbeta riktlinjer för undantag.

Praktiska konsekvenser av Datainspektionens beslut

Det bör understrykas att frågan om tillåtligheten av whistleblower-system inte varit fråga för svensk domstolsprövning eftersom Datainspektionens beslut inte överklagats. För näringslivet är det viktigt att frågan om behandling av uppgifter om lagöverträdelser enligt 21 § PUL och frågorna om personuppgiftsansvarets omfattning i detta sammanhang utreds vidare. Det är olämpligt om en företrädare för ett svenskt dotterbolag till ett företag som lyder under SOX och tillämpliga börsregler riskerar att hamna i en omöjlig situation om denne med, en om än teoretisk, risk för straff måste välja mellan att följa PUL eller SOX.

En möjlighet för svenska dotterbolag är att införa en whistleblower-telefonlinje där informatörer kan ringa till USA och rapportera till någon som i sin tur för in de aktuella uppgifterna i ett ärendehanteringssystem. Den praktiska konsekvensen av Datainspektionens tillämpning av PUL kan därför bli att svenska dotterbolag inför telefonsystem som inte omfattas av PUL vilket innebär att det inte finns några som helst integritetsgarantier för de registrerade. Vi ställer oss frågande till om Datainspektionens tillämpning är en lämplig och rimlig tolkning av direktivet.

Henrik Bengtsson och Johan Kahn
er advokater verksamma
med IT-rätt vid
Advokatfirman Delphi i Stockholm.

Noter:

1. Datainspektionens beslut i ärende Dnr 1078-2007, Dnr 1202-2007, Dnr 1221-2007, Dnr 1442-2007, Dnr 38-2008.
2. Dworkin; Sox and Whistleblowing i *Michigan law Review* Vol 105:1757, tillgänglig på *http://www.michiganlawreview.org/archive/105/8/dworkin.pdf.*
3. Standards Relating to Listed Company, Audit Committees, Exchange Act Release Nos. 33-8220, 34-47654 and IC-26001 (Apr. 9, 2003), 68 Fed. Reg. 18,788 (Apr. 16, 2003).
4. En samrådsgrupp mellan europeiske dataskyddsmyndigheter som bl a lämnar rekommendationer kring dataskyddsfrågor.
5. Mathiason & Wendling; Toward The End of the French Exception? Overcoming the Challenges of Establishing a Global «Whistleblower» Hotline, tillgänglig på http://www.littler.com/collateral/13130.pdf.
6. Korrespondensen finns tillgänglig på *http://www.complianceweek.com/s/documents/whistlers.pdf.*
7. Yttrande 1/2006 om tillämpningen av EU:s regler om uppgiftsskydd på interna system för uppgiftslämnande inom bokföring, intern bokförings-kontroll, revision, bekämpande av mutor samt brottslighet inom bank- och finansväsen), tillgänglig på *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_sv.pdf.*
8. RECOMMANDATION N° 01 / 2006 du 29 novembre 2006 N. Réf. : SA2 / SE / 2006 / 059 OBJET : Recommandation relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, tillgänglig på *http://www.privacycommission.be/fr/docs/Commission/2006/recommandation_01_2006.pdf.*
9. Spørgsmål om behandling af personoplysninger i forbindelse med whistleblowing, 05.12.06, Dnr 2006-42-1061, tillgänglig på *http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/spoergsmaal-om-behandling-af-personoplysninger-i-forbindelse-med-whistleblowing/.*
10. Guideline document adopted by the «Commission nationale de l'informatique et des libertés» (CNIL) on 10 November 2005 for the implementation of whistleblowing systems in compliance with the French Data Protection Act of 6 January 1978, as amended in August 2004, relating to information technology, data filing systems and liberties, tillgänglig på *http://www.cnil.fr/fileadmin/documents/uk/CNIL-recommandations-whistleblowing-VA.pdf* respektive Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, tillgänglig på *http://www.cnil.fr/index.php?id=1907.*
11. Advies vergunningaanvraag ex. art. 77 lid 2 WBP, 2006.01.16, Dnr 2004-1233, tillgänglig på *http://www.cbpweb.nl/downloads_adv/z2004-1233.pdf?refer=true&theme=purple.*
12. Whistleblowing – Hotlines: Internal Warning Systems and Employee Data Protection Report of the Ad-hoc Working Group on «Employee Data Protection» of the Düsseldorfer Kreis, tillgänglig på *http://info.ethicspoint.com/files/PDF/whitepapers/German_Rule_(English).pdf.*
13. Opinion 1/2006 (WP 117, s 9-13).
14. Kammarrättens i Stockholm mål nr 285-07, domen är överklagad till Regeringsrätten.
15. Ds 2007:19, s 183f.