Region Stockholm

6

Riktlinjer för hantering av personuppgifter

VKN 2019-0209

Vårdens kunskapsstyrningsnämnd
Hälso- och sjukvårdsförvaltningen
Styrning och ekonomi
Lenah Hedberg

TJÄNSTEUTLÅTANDE VKN 2019-0209
2019-11-28

Vårdens
kunskapsstyrningsnämnd

Riktlinjer för hantering av personuppgifter

Ärendebeskrivning

Den 25 maj 2018 ersattes personuppgiftslagen av det EU-gemensamma Dataskyddsdirektivet (GDPR). I artikel 5 i direktivet framgår att den personuppgiftsansvarige (Vårdens kunskapsstyrningsnämnd) ska kunna visa att förordningen följs och att de registrerades rättigheter tillgodoses. Ett led i detta är att bland annat ta fram riktlinjer för hur personuppgifter får behandlas.

Beslutsunderlag

Hälso- och sjukvårdsdirektörens tjänsteutlåtande
Riktlinjer för behandling av personuppgifter i vårdens kunskapsstyrningsnämnd

Förslag till beslut

Vårdens kunskapsstyrningsnämnd beslutar följande

1. Riktlinjer för hantering av personuppgifter fastställs.

2. Hälso- och sjukvårdsdirektören får i uppdrag att besluta om eventuella revideringar av riktlinjen för hantering av personuppgifter.

Förvaltningens motivering till förslaget

Bakgrund
Regionrevisorerna genomförde i början av 2019 en granskning av hur förvaltningen hade förberett sig inför att den nya lagstiftningen (GDPR) skulle träda i kraft 25 maj 2018. Regionrevisorerna rekommenderade (2018 projekt ID: 1502) att vårdens kunskapsstyrningsnämnd bör fastställa ett sammanhållet dokument som beskriver nämndens hantering av personuppgifter.

Överväganden
För att kunna påvisa lagefterlevnaden och ge förutsättningar för att kunna säkerställa att personuppgifter behandlas korrekt och lagligt, föreslår förvaltningen att vårdens kunskapsstyrningsnämnd enligt Europaparlamentets och rådets förordning (EU) 2016/679 Artikel 5 samt för att möta regionrevisorernas rekommendation besluta att godkänna riktlinjen.

Ekonomiska konsekvenser
Beslutet i sig förväntas få oförändrade ekonomiska konsekvenser.

Konsekvenser för patientsäkerhet
Beslutet förväntas få positiva konsekvenser för patientsäkerheten.

Konsekvenser för jämlik och jämställd vård
Beslutet förväntas få oförändrade konsekvenser för jämlik och jämställd vård.

Miljökonsekvenser
Beslutet får oförändrade konsekvenser för miljön

Administrativa konsekvenser
Beslutet förväntas få oförändrade administrativa konsekvenser för vårdgivarna då riktlinjen endast berör personuppgiftsbehandlingar i vårdens kunskapsstyrningsnämnd.

Magnus Thyberg
Avdelningschef

Margareta Tufvesson
Avdelningschef

Beslutet ska skickas till
Akten

Godkänd av Magnus Thyberg, 2019-11-28

Riktlinje för hantering av personuppgifter

Vårdens kunskapsstyrningsnämnd

Hälso- och sjukvårdsförvaltningen
08-123 132 00
Datum: 2019-10-17
Diarienummer: VKN 2019-0209

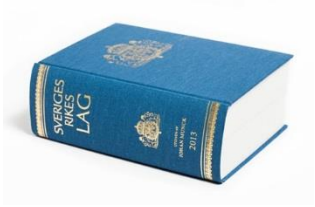
Region Stockholm

Dokumenttyp	Fastställd dat	Version:
Styrande – Tillämpning	2019-xx-xx	1.0
Fastställd av	Upprättad av	
Vårdens kunskapsstyrningsnämnd	Dataskyddsombuden VKN/HSN	

Innehållsförteckning

1 Kort om förordningen 3
1.1 Vad är en personuppgift? 4
1.1.1 Känsliga personuppgifter 4
1.2 Visa att principerna följs 5
2 Konsekvensbedömning av personuppgiftsbehandlingen 5
3 Registrera personuppgiftsbehandling 6
3.1 Vad ska rapporteras till registret? 6
3.1.1 Ansvarig kontaktperson 6
3.1.2 Kategorier av de registrerade, personuppgifter och mottagare 6
3.1.3 Ändamålet med behandlingen 7
3.1.4 Rättslig grund för behandlingen 7
3.1.5 Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna 8
3.1.6 Behörighet och loggning 9
3.1.7 Bevarande/gallring av personuppgifter 9
4 Rapportera personuppgiftsincidenter 9
4.1 Så här rapporteras en incident 10
5 Informationsplikt 10
5.1 Registerutdrag 11
6 Personuppgiftsbiträdesavtal 11
7 Personuppgifter i e-post 12

1 Kort om förordningen



Hela EU/EES har samma lagstiftning som reglerar hur man får behandla personuppgifter – Dataskyddsförordningen (GDPR).

Syftet med lagen är att stärka personers grundläggande fri- och rättigheter och särskilt skyddet av personuppgifter.

- Den som behandlar uppgifterna ska kunna visa att lagen följs
- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
- Uppgifterna ska samlas in för ett särskilt ändamål
- Uppgifterna ska vara korrekta
- Uppgifterna ska lagras så kort tid som möjligt
- Uppgifterna ska skyddas på ett korrekt sätt

Lagen anger också att de registrerade ska få tydlig information om hur deras personuppgifter hanteras. En individ vars personuppgifter hanteras har rätt att få:

- Tillgång till sin information
- Veta vad uppgifterna används till (ändamål)
- Sina uppgifter rättade om de anses felaktiga
- Sina uppgifter raderade – rätten att bli glömd[1]

En myndighet som samlar in och behandlar personuppgifter ska därför:

- Tillmötesgå förfrågningar från individen, exempelvis tillhandahålla registerutdrag
- Informera individen vid insamling och behandling av personuppgifter
- Dokumentera behandlingar i en registerförteckning
- Rapportera personuppgiftsincidenter inom 72 timmar
- Ha ett inbyggt dataskydd i system och processer

Den juridiska personen Region Stockholm och dess nämnder är ytterst ansvariga för all hantering av personuppgifter som sker inom organisationen. Alla förvaltningar och dess medarbetare ansvarar för att säkerställa att personuppgifter behandlas i enlighet med dataskyddsförordningen och annan lagstiftning.

[1] Den rättsliga grunden för personuppgiftsbehandlingen begränsar de registrerades rätt att bli glömd/ raderad.

I enlighet med lagen har varje nämnd en skyldighet att utse Dataskyddsombud, som bland annat ska:

- övervaka att organisationen följer dataskyddsförordningen
- ge råd om konsekvensbedömningar
- vara kontaktperson för de registrerade och personalen inom organisationen
- samarbeta med och vara kontaktperson till Datainspektionen.

Om personuppgifterna inte hanteras på ett lagligt och korrekt sätt kan sanktionsavgift utdömas av Datainspektionen som är tillsynsmyndighet. Även de registrerade kan begära skadestånd/ersättning av ansvarig nämnd.

1.1 Vad är en personuppgift?



Personuppgifter är all information som direkt eller indirekt kan knytas till en person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ett organisationsnummer är en personuppgift om det handlar om en enskild firma. Registreringsnumret på en bil är en personuppgift om det går att knyta till en person, medan registreringsnumret på en firmabil som används av flera anställda, inte är en personuppgift. I vissa fall räknas även olika slags elektroniska identiteter, som exempelvis IP-adress, som personuppgifter om de kan kopplas till en viss person.

1.1.1 Känsliga personuppgifter

I dataskyddsförordningen skiljer man mellan vanliga personuppgifter och känsliga personuppgifter[2]. Med känsliga personuppgifter menas:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska[3] uppgifter som entydigt identifierar en person.

[2] I dataskyddsförordningen benämns känsliga personuppgifter som särskilda kategorier av personuppgifter.

3 Biometriska data används då man använder olika matematiska och statistiska metoder för att känna igen en person baserat på en fysiologisk eller beteendemässig egenskap. Exempelvis ansiktet, fingeravtryck, handavtryck, handskrift, ögats iris.

Det är förbjudet att registrera känsliga uppgifter såvida de inte omfattas av undantag för sådan registrering, se rubrik 3.1.4.

1.2 Visa att principerna följs

Nämnden ska kunna visa att dataskyddsförordningen följs, vilket innebär att omvänd bevisbörda tillämpas. Datainspektionen (som är tillsynsmyndighet) behöver inte visa att nämnden gjort fel, utan nämnden måste istället visa att den gjort rätt.

Denna riktlinje beskriver vad och hur nämnden ska arbeta med personuppgiftsbehandlingar för att tillgodose efterlevnaden av lagkraven.

2 Konsekvensbedömning av personuppgiftsbehandlingen



En effektiv och säker användning av information är en förutsättning för Region Stockholms verksamhet och för förtroendet för regionens förmåga att leverera service till medborgarna.

Vid nya personuppgiftsbehandlingar ska ansvarig kontaktperson bedöma om det föreligger en hög risk för de registrerades integritet. Om behandlingen bedöms innebära en hög risk ska en konsekvensbedömning genomföras. Den personuppgiftsansvarige ansvarar för att konsekvensbedömningen genomförs innan personuppgifter börjar behandlas, tillsammans med eventuella personuppgiftsbiträden och Dataskyddsombudet.

Det finns fyra grundläggande krav på vad en konsekvensbedömning ska innehålla:

1. En systematisk beskrivning av den planerade behandlingen och behandlingens syfte. I denna beskrivning ska bland annat ändamålet, den lagliga grunden, lagringstiden, och omfattningen av flödet av personuppgifter i behandlingen dokumenteras.
2. En bedömning av om behandlingen är nödvändig och insamlingen av information står i proportion i förhållande till angivet ändamål.
3. Hot och risker med behandlingen ska identifieras. Dess konsekvenser samt sannolikhetsgraden för att de inträffar ska bedömas.
4. Även åtgärder för att minimera riskerna ska fastställas och dokumenteras som en del i att kunna påvisa efterlevnaden av lagen.

Kontakta Dataskyddsombudet för samråd vid konsekvensbedömning.

3 Registrera personuppgiftsbehandling



Alla personuppgiftsansvariga (respektive nämnd) ansvarar för sina personuppgiftsbehandlingar och har skyldighet att föra ett register över dem. Här registreras alla behandlingar, både det som sker i system och manuellt.

Dataskyddförordningen ställer krav på att vissa förutsättningar måste uppfyllas för att personuppgiftsbehandlingen ska vara laglig. Kraven ska finnas dokumenterade i registret, vilka beskrivs utförligare i detta dokument.

3.1 Vad ska rapporteras till registret?

Det finns ett antal informationsmängder som ska finnas dokumenterade i registret:

- Ansvarig kontaktperson för behandlingen
- Kategorier av registrerade, av personuppgifter och av mottagare
- Ändamål med behandlingen
- Rättslig grund för behandlingen
- Tidsintervall för bevarande/gallring
- Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna

3.1.1 Ansvarig kontaktperson

Även om nämnden är personuppgiftsansvarig ska det alltid finns en ansvarig kontaktperson i linjeorganisationen som ansvarar för behandlingen och säkerställer efterlevnaden av lagstiftningen. I händelse av att en personuppgiftsincident inträffar, se kapitel 4, är det också viktigt att kontaktuppgifter är uppdaterade så att man snabbt kan komma i kontakt med ansvarig person.

3.1.2 Kategorier av de registrerade, personuppgifter och mottagare

Alla typer av personuppgifter ska specificeras och dokumenteras. Detta gäller även de som på uppdrag av den personuppgiftsansvarige behandlar personuppgifter eller de som personuppgifterna skickas till. I registerförteckningen ska därför anges;

1. Kategorier av de som registreras. Med detta avses exempelvis patienter anställda/medarbetare, medlemmar etc.
2. Vilka personuppgifter som registreras. Med detta avses exempelvis namn, kontaktuppgifter, personnummer, uppgifter om hälsa, diarienummer, IP-adress etc.

3. Vilka som kommer att ta del av informationen. Med detta avses till vilka personuppgifterna lämnas ut till, exempelvis Socialstyrelsen, SKL, Skatteverket, namngivet personuppgiftsbiträde etc.

3.1.3 Ändamålet med behandlingen

Personuppgifter får endast samlas in för ett särskilt ändamål, och syftet med den aktuella personuppgiftsbehandlingen ska dokumenteras och tydligt beskrivas i registerförteckningen. Uppgifterna får inte användas på något annat sätt än vad som angavs i ändamålet när anmälan gjordes. Detta innebär att inga fler uppgifter än nödvändigt för att tillgodose ändamålet, får samlas in.

Tänk på att det inte är syftet med IT-systemet, utan syftet med personuppgiftsbehandlingen som ska dokumenteras.

3.1.4 Rättslig grund för behandlingen

Alla personuppgiftsbehandlingar måste ha rättslig grund annars är den olaglig. Det finns sex rättsliga grunder i dataskyddsförordningen som kan vara aktuella för personuppgiftsbehandlingar. Inom nämnden, används huvudsakligen nedanstående angivna rättsliga grunder:

- **Rättslig förpliktelse**: Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet.
- **Myndighetsutövning och uppgift av allmänt intresse**: Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.
- **Avtal**: Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige, exempelvis anställningsavtal.
- **Samtycke:** Den registrerade har sagt ja till personuppgiftsbehandlingen.

Den rättsliga grunden samtycke bör endast användas *i undantagsfall*. Samtycket kan återkallas och den registrerade kan begära att uppgifterna raderas, vilket måste ske om samtycke är enda grunden för behandlingen. Samtycke kan bara användas när det verkligen föreligger ett fritt val för den registrerade. Ett exempel på det är deltagande i *forskningsprojekt*. Verksamheten har ansvar för att visa att den registrerade har fått tydlig information och gjort ett fritt och aktivt val att samtycka.

Behandling av känsliga personuppgifter är i grunden olagligt men nämndens uppdrag möjliggör att känsliga personuppgifter får behandlas i enlighet med undantagen i art 9.2 dataskyddsförordningen[4], under förutsättning att det finns ett tydligt ändamål som motiverar insamlingen av uppgifterna som behandlas, se 2.1.3.

[4] Läs mer i dataskyddsförordningen här

3.1.5 Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna

För att kunna dokumentera de vidtagna tekniska och organisatoriska säkerhets-åtgärderna i registerförteckningen ska ansvarig säkerställa efterlevnaden av Region Stockholms policy och riktlinje för informationssäkerhet.

I enlighet med riktlinjen för informationssäkerhet ansvarar informationsägaren för att informationssäkerhet i enlighet med de krav som ställs i lagstiftning och regionens regelverk kring informationssäkerhet uppnås i det IT-system som systemägaren ansvarar för. Personuppgifter ska vara korrekta och uppdaterade. Den som behandlar personuppgifter måste se till att rätta eller radera felaktiga uppgifter omgående.

Det är informationsägaren som ska klassificera informationen, bedöma risker och ställa säkerhetskrav, eftersom det är hos denne som konsekvenserna av bristande informationssäkerhet kan uppstå. Systemsäkerhet kräver ett samarbete mellan flera olika kompetenser, både någon från verksamheten som kan arbetsprocessen och vilka krav som finns och någon som har IT-kompetens och känner till vilka krav som ställs på IT-system.

- Informationssäkerhetsklassning genomförs för att veta vilken typ av information systemet hanterar och vilka krav som ställs på hantering av denna. Informationen ska klassas utifrån konfidentialitet, riktighet, och tillgänglighet.
- Regelefterlevnad: Baserat på hur informationen klassats analyseras de krav som ställs på systemet[5].
- Riskanalyser: Identifiering och bedömning av risker vars konsekvenser kan leda till störningar i informationstillgången, allvarliga händelser eller extraordinära händelser. Föreligger en hög risk för den registrerades integritet ska en konsekvensbedömning genomföras, enligt kap 2. Syftet är att visa att personuppgiftsansvarig har vidtagit tillräckliga åtgärder för att skydda den registrerades integritet och rättigheter.

[5] Läs mer om informationsklassning här.

3.1.6 Behörighet och loggning

Säkerhetskraven på IT-system som hanterar personuppgifter stärks genom lagstiftningen. Personuppgifter ska exempelvis skyddas så att bara de som är behöriga kan se eller arbeta med uppgifterna. Uppgifterna måste även skyddas så de inte förstörs genom olyckshändelse.

Ett grundkrav på system som innehåller personuppgifter är att de går att behörighetsstyra. Säkerheten kring behörigheter beror mycket på tilldelning och avslutande av behörigheter. Om det dessutom gäller tillgång till känsliga personuppgifter är kraven ännu högre på fungerande rutiner för behörighetshantering och även loggningsfunktioner i systemen, till exempel vem som gjorde vad och när.

Det behöver finnas arbetsrutiner för behörigheter:

- Säkerställ att verksamheten har fungerande rutiner även när en medarbetare byter tjänst internt.
- Ha rutiner för att minst årligen kontrollera att behörigheterna är korrekta.
- Kraven på behörigheter gäller även samtliga leverantörer och andra externa användare. Se därför regelbundet över vilka behörighet som finns.

3.1.7 Bevarande/gallring av personuppgifter

Bevarande/gallringsplaner måste finnas för alla personuppgiftsbehandlingar som genomförs i förvaltningen. För mer information om bevarande- och gallringsplaner kontakta regionarkivet[6].

4 Rapportera personuppgifts-incidenter



En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel på incidenter:

[6] Kontakt till regionarkivet https://www.regionarkivet.sll.se/

- Någon har kommit över ett lösenord som gör att den skulle kunna logga in i system som behandlar personuppgifter.
- Ett mejl med känsliga eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- Ett glömt papper i skrivare som innehåller uppgifter om namn och sjukdomstillstånd.
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.

4.1 Så här rapporteras en incident

För att utreda om personuppgiftsincidenten har skett krävs först en utredning av säkerhetsincidenten i enlighet med riktlinjen för Informationssäkerhet rubrik 12.1. Riktlinjen anger bland annat att akuta IT-incidenter som kräver omedelbara åtgärder ska rapporteras till IT-driftorganisationen, till exempel via verksamhetens IT-support. IT- incidenter som innebär att en utrednings- eller åtgärdsfas behöver påbörjas ska snarast rapporteras till systemägaren/enhetschef som i sin tur informerar informationsägaren/ avdelningschefen. Även informationssäkerhetssamordnare ska engageras i enligt med anvisade rutiner.

Om incidenten berör personuppgifter ska ansvarigt dataskyddsombud kontaktas för bedömning för vidare hantering av ärendet.

Alla personuppgiftsincidenter ska rapporteras och dokumenteras. Det är viktigt för att vi ska kunna agera vid både allvarliga och mindre allvarliga brister. Varje medarbetare ansvarar för att rapportera och dokumentera risk för, misstanke om eller inträffande av en personuppgiftsincident. Om incidenten bedöms utgöra en hög risk för de registrerades fri- och rättigheter ska personuppgiftsincidenten anmälas till Datainspektionen inom 72 timmar efter att den har upptäckts. Därför är det angeläget att utredningen görs skyndsamt. Anmälan görs av ansvarig kontaktperson i samråd med Dataskyddsombudet. Detta gäller även om incidenten inträffat hos ett av våra biträden, det vill säga någon av våra leverantörer. Därför är det viktigt att varje medarbetare rapporterar inträffad personuppgiftsincident.

5 Informationsplikt



Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

5.1 Registerutdrag

Varje medborgare har rätt att få veta om myndigheten behandlar dennes personuppgifter. Personuppgiftsansvarig är skyldig att, vid förfrågan, ge ut dessa uppgifter till medborgaren genom ett så kallat registerutdrag.

Ett registerutdrag inkluderar både strukturerade och ostrukturerade data (Word-filer, Excel-filer, enklare listor etcetera). Undantag finns; ett registerutdrag omfattar till exempel inte personuppgifter som finns i löpande text som utgör ett utkast eller en minnesanteckning.

Informationen ska som regel tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. Följande information ska lämnas:

- Vem som är personuppgiftsansvarig.
- Kontaktuppgifter till Dataskyddsombudet.
- Ändamålen med behandlingen.
- Den rättsliga grunden för behandlingen.
- Vilka som har tillgång till uppgifterna.
- Den period som personuppgifterna kommer att lagras.
- Rätten att korrigera felaktiga uppgifter.
- Möjligheten att kontakta Datainspektionen som är tillsynsmyndighet.

6 Personuppgiftsbiträdesavtal



Den som samlar in personuppgifter med stöd av en rättslig grund är personuppgiftsansvarig (PuA). Personuppgiftsansvarig ansvarar för vilken data som samlas in och på vilket sätt den ska hanteras. Personuppgiftsbiträde (PuB) är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Till huvudavtalet med leverantör som behandlar personuppgifter för den personuppgiftsansvariges räkning ska ett PuB-avtal tecknas som en bilaga till huvudavtalet. I PuB-avtalet ska det även framgå i en instruktion på vilket sätt personuppgifterna får behandlas av biträdet[7].

Varje verksamhet ansvarar för att PuB-avtal ingås med samtliga leverantörer och externa aktörer där personuppgifter överlämnas för behandling.

PUB-avtal som upprättats innan 25 maj 2018 ska uppdateras.

[7] PUB- avtal

7 Personuppgifter i e-post



Hantering av personuppgifter ska främst ske i system, inte i e-post. Användaren ska betrakta e-post som oskyddad och Region Stockholms nätverk som öppna (osäkra). Detta innebär att meddelanden som skickas okrypterade via e-post inte kan betraktas vara skyddade från insyn, och att det därmed finns risk för att andra än den avsedda mottagaren kan ta del av innehållet.

I e-posten får du inte alls behandla eller spara personuppgifter som är **känsliga eller sekretessbelagda**. Om känsliga eller sekretessbelagda personuppgifter inkommer kan du till exempel inte vidarebefordra eller svara på mejlet när det innehåller uppgifterna. Flytta över informationen till lämpligt system och radera mailet omgående. Observera att personuppgifterna ska tas bort i inkorgen, skickat-mappen och i borttaget.

Om det kommer ett e-postmeddelande med icke känsliga personuppgifter ska dessa alltid behandlas varsamt. Exempel är namn, adress, telefonnummer etcetera. Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum. Spara aldrig mejl med personuppgifter i Outlook "för att det kan vara bra att ha". Informera alla anställda inom din verksamhet om ovanstående punkter.

För mer information om dataskyddsförordningen:

https://www.datainspektionen.se/

https://skl.se/ekonomijuridikstatistik/juridik/offentlighetsekretessarkiv/dataskyddsforordningengdpr.13023.html

https://intranat.sll.se/stod-i-arbetet/juridik/nya-dataskyddsforordningen---gdpr/